EVROPSKA
KOMISIJA

Bruselj, 29.5.2019
COM(2019) 250 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Smernice k uredbi o okviru za prosti pretok neosebnih podatkov v Evropski uniji

Kazalo

1 Uvod ... 2

Namen teh smernic ... 3

2 Medsebojni vpliv med uredbo o prostem pretoku neosebnih podatkov in splošno uredbo o varstvu podatkov – mešani podatkovni nizi ... 4

2.1 Pojem neosebnih podatkov v uredbi o prostem pretoku neosebnih podatkov ... 4

Osebni podatki ... 4

Neosebni podatki ... 5

2.2 Mešani podatkovni nizi ... 7

3 Prosti pretok podatkov in odprava zahtev glede lokalizacije podatkov ... 10

3.1 Prosti pretok neosebnih podatkov ... 10

3.2 Prosti pretok osebnih podatkov ... 12

3.3 Področje uporabe uredbe o prostem pretoku neosebnih podatkov ... 13

3.4 Dejavnosti v zvezi z notranjo organizacijo držav članic ... 14

4 Samoregulativni pristopi, ki podpirajo prosti pretok podatkov ... 15

4.1 Prenos podatkov in zamenjava ponudnikov storitev v oblaku ... 15

Pojem prenosljivosti in medsebojno vplivanje s splošno uredbo o varstvu podatkov ... 16

4.2 Kodeksi ravnanja in certifikacijske sheme v zvezi z varstvom osebnih podatkov ... 18

4.3 Spodbujanje zaupanja v čezmejno obdelavo podatkov – certificiranje varnosti ... 19

Končne pripombe ... 19

Evropska komisija je ta dokument pripravila zgolj za informativne namene. Dokument ne vsebuje verodostojne razlage Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji in ne pomeni sklepa ali stališča Evropske komisije. Ne posega v noben tovrsten sklep ali stališče Evropske komisije niti v pooblastila Sodišča EU za razlaganje navedene uredbe v skladu s Pogodbama EU.

1 Uvod

V gospodarstvu, ki je vse bolj podatkovno vodeno, so tokovi podatkov v središču poslovnih procesov v podjetjih vseh velikosti in v vseh sektorjih. Nove digitalne tehnologije prinašajo nove priložnosti za splošno javnost, podjetja in javne uprave v Evropski uniji (v nadaljnjem besedilu: EU).

Evropski parlament in Svet sta za nadaljnje povečanje čezmejne izmenjave podatkov in spodbuditev podatkovnega gospodarstva novembra 2018 na podlagi predloga Evropske komisije (v nadaljnjem besedilu: Komisija) sprejela Uredbo (EU) 2018/1807 o okviru za prosti pretok neosebnih podatkov v Evropski uniji[1] (v nadaljnjem besedilu: uredba o prostem pretoku neosebnih podatkov). Uredba se uporablja od 28. maja 2019. Načelo prostega pretoka osebnih podatkov je že določeno v Uredbi (EU) 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljnjem besedilu: splošna uredba o varstvu podatkov)[2]. Zato je zdaj vzpostavljen celovit okvir za skupni evropski podatkovni prostor in prosti pretok vseh podatkov v Evropski uniji[3].

Uredba o prostem pretoku neosebnih podatkov podjetjem zagotavlja pravno varnost, da lahko svoje podatke v EU obdelujejo, kjer koli želijo, povečuje zaupanje v storitve obdelave podatkov in preprečuje prakse, ki povzročajo vezanost na ponudnika. S tem se bo povečala možnost izbire za potrošnike, izboljšala učinkovitost in spodbudilo uvajanje tehnologij v oblaku, kar bo podjetjem v EU omogočilo velike prihranke. Študija kaže, da lahko podjetja v EU s prehodom na računalništvo v oblaku prihranijo 2050 % stroškov za informacijsko tehnologijo[4].

Zaradi obeh uredb se lahko podatki prosto pretakajo med državami članicami, kar uporabnikom storitev obdelave podatkov omogoča, da podatke, zbrane na različnih trgih EU, uporabljajo za izboljšanje svoje produktivnosti in konkurenčnosti. Tako lahko uporabniki v celoti izkoristijo ekonomije obsega, ki jih zagotavlja velik trg EU, s čimer izboljšajo svojo globalno konkurenčnost, poveča pa se tudi medsebojna povezanost evropskega podatkovnega gospodarstva.

Uredba o prostem pretoku neosebnih podatkov ima tri pomembne značilnosti:

- državam članicam praviloma prepoveduje uvedbo zahtev glede lokalizacije podatkov. Izjeme od tega pravila so lahko utemeljene le na podlagi javne varnosti ob upoštevanju načela sorazmernosti;
- vzpostavlja mehanizem sodelovanja za zagotovitev, da bodo lahko pristojni organi še naprej uveljavljali vse pravice do dostopa do podatkov, ki se obdelujejo v drugi državi članici;
- Industriji daje spodbude, da ob podpori Komisije oblikuje samoregulativne kodekse ravnanja glede zamenjave ponudnikov storitev in prenosa podatkov.

---

[1] Uredba (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji, UL L 303, 28.11.2018, str. 59.

[2] 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), UL L 119, 4.5.2016, str. 1.

[3] Splošna uredba o varstvu podatkov velja tudi za Evropski gospodarski prostor (EGP), ki vključuje Islandijo, Lihtenštajn in Norveško. Poleg tega je uredba o prostem pretoku neosebnih podatkov označena kot besedilo, ki velja za EGP.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe* (Merjenje gospodarskega vpliva računalništva v oblaku v Evropi), SMART 2014/0031, 2016. Na voljo na spletnem naslovu: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

Namen teh smernic

Te smernice izpolnjujejo zahtevo iz člena 8(3) uredbe o prostem pretoku neosebnih podatkov, v skladu s katerim mora Komisija objaviti smernice o medsebojnem vplivu med to uredbo in splošno uredbo o varstvu podatkov, „zlasti kar zadeva podatkovne nize, ki vsebujejo osebne in neosebne podatke“.

Namen teh smernic je uporabnikom – zlasti malim in srednjim podjetjem – pomagati razumeti medsebojni vpliv med uredbo o prostem pretoku neosebnih podatkov in splošno uredbo o varstvu podatkov[5]. Zato smernice obravnavajo zlasti: (i) pojma neosebnih in osebnih podatkov; (ii) načeli prostega pretoka podatkov in prepovedi zahtev glede lokalizacije podatkov v skladu z obema uredbama ter (iii) pojem prenosljivosti podatkov v skladu z uredbo o prostem pretoku neosebnih podatkov. Zajemajo tudi samoregulativne zahteve iz obeh uredb.

Uredba o prostem pretoku neosebnih podatkov zajema samo „podatke, ki niso osebni podatki“, kot so opredeljeni v splošni uredbi o varstvu podatkov. Splošna uredba o varstvu podatkov ureja obdelavo osebnih podatkov in je bistveni del okvira EU za varstvo podatkov[6]. V državah članicah je začela veljati 25. maja 2018. Uredba določa usklajena pravila o varstvu ljudi v EU/EGP pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Splošna uredba o varstvu podatkov: (i) med drugim določa, katere informacije so osebni podatki; (ii) vzpostavlja pravno podlago za njihovo obdelavo ter (iii) opredeljuje pravice in obveznosti, ki jih je treba upoštevati pri obdelavi teh podatkov[7]. Kar zadeva načelo prostega pretoka osebnih podatkov, člen 1(3) splošne uredbe o varstvu podatkov določa, da

---

[5] Uvodna izjava 37 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[6]
- 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), UL L 119/1, 4.5.2016, str. 1.
- Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES, UL L 295, 21.11.2018, str. 39.
- Direktiva (EU) 2016/680 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, UL L 119, 4.5.2016, str. 89.
- Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), UL L 201, 31.7.2002, str. 37 (trenutno v reviziji).

[7] Več smernic o različnih vidikih 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 (Splošna uredba o varstvu podatkov) in evropski zakonodaji o varstvu podatkov je na voljo na spletni strani Evropskega odbora za varstvo podatkov, ki je v skladu s členom 70 splošne uredbe o varstvu podatkov izdal več smernic, ki so na voljo na spletnem naslovu: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_sl. Na zadevni spletni strani so tudi sklici na smernice, priporočila in druge dokumente, ki jih je izdala predhodnica Evropskega odbora za varstvo podatkov, tj. delovna skupina iz člena 29. Poleg tega je Komisija za ozaveščanje državljanov in podjetij o Uredbi (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) izdala sporočilo o varstvu podatkov, ki vsebuje navodila o neposredni uporabi splošne uredbe o varstvu podatkov (COM(2018)43 final) in je na voljo na spletnem naslovu: https://eur-lex.europa.eu/legal-content/SL/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

„[p]rosti pretok osebnih podatkov v Uniji ne sme biti omejen ali prepovedan iz razlogov, povezanih z varstvom posameznikov pri obdelavi osebnih podatkov.“

V večini primerov iz resničnega življenja je podatkovni niz zelo verjetno sestavljen iz osebnih in neosebnih podatkov. To se pogosto imenuje „mešani podatkovni niz“. Medsebojni vpliv med uredbo o prostem pretoku neosebnih podatkov in splošno uredbo o varstvu podatkov je podrobneje pojasnjen v oddelku 2.2.

Splošna uredba o varstvu podatkov in uredba o prostem pretoku neosebnih podatkov zaradi jasnosti ne vsebujeta nasprotujočih si obveznosti.

2 Medsebojni vpliv med uredbo o prostem pretoku neosebnih podatkov in splošno uredbo o varstvu podatkov – mešani podatkovni nizi

2.1 Pojem neosebnih podatkov v uredbi o prostem pretoku neosebnih podatkov

Cilj uredbe o prostem pretoku neosebnih podatkov[8] je zagotoviti prosti pretok podatkov, ki niso osebni podatki. V celotnem besedilu Uredbe se uporablja pojem „podatki“, ki bi ga bilo treba razumeti kot „podatke, ki niso osebni podatki, kakor so opredeljeni v točki (1) člena 4 Uredbe (EU) 2016/679 [splošna uredba o varstvu podatkov]“[9]. Taki podatki, ki se v tem dokumentu imenujejo tudi „neosebni podatki“, so opredeljeni kot nasprotje (*a contrario*) osebnih podatkov, kakor so opredeljeni v splošni uredbi o varstvu podatkov.

Osebni podatki

V splošni uredbi o varstvu podatkov je navedeno: „osebni podatki “ pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;“.

Široka opredelitev osebnih podatkov je namerna in je v splošni uredbi o varstvu podatkov v primerjavi s prejšnjo zakonodajo ostala v bistvu nespremenjena[10]. Različne vidike opredelitve osebnih podatkov, kot so „katera koli informacija“, „v zvezi z“, „določen ali določljiv“, je obravnavala že delovna

[8] Člen 1 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[9] Glej člen 3(1) Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[10] Glej člen 2(a) Direktive 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 (datum izteka veljavnosti: 24. maj 2018, razveljavljena s splošno uredbo o varstvu podatkov). Glej tudi sodno prakso Sodišča o opredelitvi osebnih podatkov, s katero se priznava široka razlaga tega pojma, na primer sodbo Sodišča z dne 29. januarja 2009, *Productores de Música de España (Promusicae)* proti *Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; sodbo Sodišča z dne 24. novembra 2011, *Scarlet Extended SA* proti *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; sodbo Sodišča z dne 19. oktobra 2016, *Patrick Breyer* proti *Zvezni republiki Nemčiji*, C-582/14, ECLI:EU:C:2016:779.

skupina iz člena 29[11] v svojem mnenju 4/2007 o pojmu neosebnih podatkov z dne 20. junija 2007, WP 136.

Na področjih, kot so raziskave, se osebni podatki običajno psevdonimizirajo, da se prikrije identiteta posameznika. Psevdonimizacija je obdelava osebnih podatkov na tak način, da jih brez dodatnih informacij ni več mogoče pripisati specifični osebi. Te dodatne informacije se hranijo ločeno in so zavarovane z organizacijskimi ali tehničnimi ukrepi (npr. šifriranjem)[12,13]. Vendar pa se podatki, ki so bili psevdonimizirani, še vedno štejejo za informacije o določljivi osebi, če jih je mogoče z uporabo dodatnih informacij pripisati tej osebi[14]. Taki podatki so osebni podatki v skladu s splošno uredbo o varstvu podatkov.

Neosebni podatki

Kadar podatki niso „osebni podatki“, kakor so opredeljeni v splošni uredbi o varstvu podatkov, so neosebni. Neosebne podatke je mogoče glede na poreklo razvrstiti kot:

- prvič: podatke, ki se sprva niso nanašali na določeno ali določljivo fizično osebo, kot so podatki o vremenskih razmerah, ki jih ustvarijo senzorji, nameščeni na vetrnih turbinah, ali podatki o potrebah po vzdrževanju za industrijske stroje;

- drugič: podatke, ki so bili sprva osebni podatki, pozneje pa so bili **anonimizirani**[15]. „Anonimizacija“ osebnih podatkov se razlikuje od psevdonimizacije (glej zgoraj), saj ustrezno anonimiziranih podatkov ni mogoče pripisati določeni osebi, niti z uporabo dodatnih podatkov[16], zato so to neosebni podatki.

[11] Delovna skupina iz člena 29 je bila svetovalni organ, ki je Komisiji svetoval o zadevah v zvezi z varstvom podatkov in pomagal pri oblikovanju usklajenih politik varstva podatkov v EU. Po začetku veljavnosti splošne uredbe o varstvu podatkov 25. maja 2018 je delovno skupino iz člena 29 nasledil Evropski odbor za varstvo podatkov.

[12] Glej člen 4(5) 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 (splošna uredba o varstvu podatkov), v katerem je opredeljena „psevdonimizacija“.

[13] Raziskovalna študija o učinkih novega zdravila bi se lahko na primer štela za psevdonimizacijo, če bi se osebni podatki sodelujočih v študiji v raziskovalni dokumentaciji nadomestili z enotnimi atributi (npr. številko ali kodo), njihovi osebni podatki pa bi bili z dodeljenimi enotnimi atributi ločeno shranjeni v zavarovanem dokumentu (npr. v podatkovni bazi, zaščiteni z geslom).

[14] Glej uvodno izjavo 26 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 (splošna uredba o varstvu podatkov).

[15] Glej uvodno izjavo 26 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 (Splošna uredba o varstvu podatkov), v kateri je navedeno, da „[n]ačel varstva podatkov zato ne bi smeli uporabljati za anonimizirane informacije, in sicer informacije, ki niso povezane z določenim ali določljivim posameznikom, ali osebne podatke, ki so bili anonimizirani na tak način, da posameznik, na katerega se nanašajo osebni podatki, ni ali ni več določljiv.“

[16] Glej sodbo Sodišča z dne 19. oktobra 2016, *Patrick Breyer* proti *Zvezni republiki Nemčiji*, C-582/14, ECLI:EU:C:2016:779. Sodišče je menilo, da lahko dinamični naslov internetnega protokola (IP) pomeni osebne podatke, tudi če dodatne podatke, s katerimi bi bilo mogoče identificirati posameznika, hrani tretja oseba (npr. ponudnik internetnih storitev). Možnost identifikacije posameznika mora pomeniti sredstvo, za katero se razumno pričakuje, da se bo uporabilo za posredno ali neposredno identifikacijo posameznika.

Ocena, ali so podatki ustrezno anonimizirani, je odvisna od posebnih in edinstvenih okoliščin vsakega posameznega primera[17]. Več primerov ponovne identifikacije podatkovnih nizov, ki naj bi bili anonimizirani, je pokazalo, da je ta ocena lahko zahtevna[18]. Za ugotovitev, ali je posameznik določljiv, je treba upoštevati vsa sredstva, za katera se razumno pričakuje, da jih bosta upravljavec ali druga oseba uporabila za neposredno ali posredno določitev posameznika[19].

Primeri neosebnih podatkov

- Podatki, ki se združijo tako, da ni več mogoče določiti posameznih dogodkov (kot so posamezna potovanja osebe v tujino ali potovalni vzorci, ki bi lahko pomenili osebne podatke), se lahko štejejo za anonimne podatke[20].. Anonimni podatki se uporabljajo na primer v statistiki ali poročilih o prodaji (na primer za oceno priljubljenosti izdelka in njegovih značilnosti).
- Podatki o visokofrekvenčnem trgovanju v finančnem sektorju ali podatki o preciznem kmetovanju, ki pomagajo spremljati in optimizirati uporabo pesticidov, hranil in vode.

Če pa je mogoče neosebne podatke kakor koli povezati s posameznikom, zaradi česar je ta posameznik neposredno ali posredno določljiv, jih je treba šteti za osebne podatke.

Če na primer poročilo o nadzoru kakovosti na proizvodni liniji omogoča, da se podatki povežejo z določenimi tovarniškimi delavci (npr. tistimi, ki nastavljajo proizvodne parametre), bi se ti podatki šteli za osebne podatke, zato je treba uporabljati splošno uredbo o varstvu podatkov. Enaka pravila veljajo, če razvoj tehnologije in podatkovne analitike omogoča pretvorbo anonimiziranih podatkov v osebne podatke. [21]

---

[17] Podatke bi bilo treba vedno anonimizirati z najsodobnejšimi tehnikami anonimizacije.

[18] Primeri ponovne identifikacije podatkov, ki naj bi bili anonimizirani, so na voljo v študiji o prihodnjih tokovih podatkov, ki sta jo za Odbor Evropskega parlamenta za industrijo, raziskave in energetiko (ITRE) izvedla Blackman, C., in Forge, S.: *Data Flows – Future Scenarios: In-Depth Analysis for the ITRE Committee* (Tokovi podatkov – prihodnji scenariji: poglobljena analiza za odbor ITRE), 2017, str. 22, okvir 2. Na voljo na spletnem naslovu: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf.

[19] Glej uvodno izjavo 26 Uredbe (EU) 2016/679 (splošna uredba o varstvu podatkov), v skladu s katero bi bilo treba za ugotovitev, „ali se za ta sredstva lahko razumno pričakuje, da bodo uporabljena za identifikacijo posameznika, […] upoštevati vse objektivne dejavnike, kot so stroški identifikacije in čas, potreben zanjo, ter pri tem upoštevati razpoložljivo tehnologijo in tehnološki razvoj v času obdelave“.

[20] Glej mnenje delovne skupine iz člena 29: Mnenje št. 5/2014 o anonimizacijskih tehnikah, sprejeto 10. aprila 2014, WP216, str. 9: „Nastali nabor podatkov bi bilo mogoče opredeliti kot anonimen samo, če bi upravljavec podatkov te podatke združil tako, da posamezni dogodki ne bi bili več določljivi. Na primer: če organizacija zbira podatke o potovalnih premikih posameznikov, bi potovalni vzorci posameznikov na ravni dogodka še vedno izpolnjevali pogoje za osebne podatke za katero koli osebo, vse dokler bi imel upravljavec podatkov (ali katera koli druga oseba) še vedno dostop do prvotnih surovih podatkov, tudi če so bili neposredni identifikatorji odstranjeni iz nabora podatkov, predloženega tretjim osebam. Če pa bi upravljavec podatkov izbrisal surove podatke in tretjim osebam predložil samo zbirne statistične podatke na visoki ravni, kot na primer „ob ponedeljkih je na poti X 160 % več potnikov kot ob torkih“, bi se ti podatki šteli za anonimne.“

[21] Če se osebni podatki obdelujejo nezakonito ali se z njihovo obdelavo drugače krši splošna uredba o varstvu podatkov, imajo posamezniki, na katere se nanašajo osebni podatki (fizične osebe), v skladu s splošno uredbo o varstvu podatkov pravico vložiti pritožbo pri nacionalnem nadzornem organu (organu za varstvo podatkov) v EU ali uveljavljati učinkovito pravno sredstvo pred nacionalnim sodiščem. Naloge, pristojnosti in pooblastila nacionalnih nadzornih organov ureja oddelek 2 poglavja VI splošne uredbe o varstvu podatkov.

Ker se opredelitev osebnih podatkov nanaša na „posameznike“, so podatkovni nizi, ki vsebujejo imena in kontaktne podatke pravnih oseb, načeloma neosebni podatki[22]. Vendar so to lahko v nekaterih primerih osebni podatki[23]. To velja, če je na primer ime pravne osebe enako imenu fizične osebe, ki je njena lastnica, ali če se informacija nanaša na določeno ali določljivo fizično osebo[24].

2.2 Mešani podatkovni nizi

Uredba o prostem pretoku neosebnih podatkov in splošna uredba o varstvu podatkov vsebujeta različna pristopa k prostemu pretoku podatkov v EU.

Uredba o prostem pretoku neosebnih podatkov določa splošno prepoved zahtev glede lokalizacije podatkov za neosebne podatke. S členom 4(1) Uredbe so prepovedane zahteve glede lokalizacije podatkov, razen če so utemeljene na podlagi javne varnosti ob upoštevanju načela sorazmernosti.

Splošna uredba o varstvu podatkov poleg visoke ravni varstva osebnih podatkov zagotavlja tudi prosti pretok osebnih podatkov. V skladu s členom 1(3) Uredbe prosti pretok osebnih podatkov „ne sme biti omejen ali prepovedan iz razlogov, povezanih z varstvom posameznikov pri obdelavi osebnih podatkov“. Uredbi skupaj zagotavljata prosti pretok „vseh“ podatkov znotraj EU. Posebne določbe so podrobneje obravnavane v oddelkih 3.1 in 3.2.

Mešani podatkovni niz je sestavljen iz osebnih in neosebnih podatkov. Mešani podatkovni nizi predstavljajo večino podatkovnih nizov, ki se uporabljajo v podatkovnem gospodarstvu, in so pogosti zaradi tehnoloških dosežkov, kot so internet stvari (tj. digitalno povezovanje objektov), umetna inteligenca in tehnologije, ki omogočajo analizo velepodatkov.

Primeri mešanih podatkovnih nizov:

- davčna evidenca podjetja, v kateri sta navedena ime in telefonska številka izvršnega direktorja podjetja;
- podatkovni nizi v banki, zlasti tisti, ki vsebujejo podatke o strankah in podrobnosti o transakcijah, kot so plačilne storitve (kreditne in debetne kartice), aplikacije za upravljanje odnosov s partnerji (*partner relationship management* – PRM) in posojilne pogodbe, dokumenti, v katerih so združeni podatki o fizičnih in pravnih osebah;
- anonimizirani statistični podatki raziskovalne ustanove in prvotno zbrani surovi podatki, kot so odgovori posameznih udeležencev na vprašanja v okviru statističnih raziskav;
- zbirka znanja podjetja o težavah z informacijsko tehnologijo (IT) in rešitvah zanje na podlagi posameznih poročil o incidentih v zvezi z IT;

[22] V uvodni izjavi 14 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 (splošna uredba o varstvu podatkov) je navedeno: „Ta uredba ne zajema obdelave osebnih podatkov glede pravnih oseb in zlasti družb, ustanovljenih kot pravne osebe, vključno z imenom in obliko ter kontaktnimi podatki pravne osebe.“ Vendar pa je treba pri branju navedenega upoštevati opredelitev osebnih podatkov iz člena 4(1) splošne uredbe o varstvu podatkov.

[23] Glej sodbo Sodišča z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR*, C-92/09 in *Hartmut Eifert*, C-93/09 proti *Land Hessen*, ECLI:EU:C:2010:662, točka 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en

- podatki, povezani z internetom stvari, če nekateri med njimi omogočajo oblikovanje predpostavk o določljivih posameznikih (npr. prisotnost na določenem naslovu in vzorci uporabe), ter
- analiza podatkov iz operativnih dnevnikov za proizvodno opremo v predelovalni industriji.

Primer: storitve upravljanja odnosov s strankami

Nekatere banke uporabljajo storitve upravljanja odnosov s strankami (*customer relationship management* – CRM), ki jih zagotavljajo tretje osebe in pri katerih morajo biti podatki stranke na voljo v okolju CRM. Podatki, hranjeni v storitvi CRM, bodo vključevali vse informacije, potrebne za učinkovito upravljanje interakcij s stranko, kot so poštni in e-poštni naslov, telefonska številka, izdelki in storitve, ki jih kupijo, ter poročila o prodaji, vključno z zbirnimi podatki. Zato lahko ti podatki vključujejo osebne in neosebne podatke o strankah.

Uredba o prostem pretoku neosebnih podatkov[25] v zvezi z mešanimi podatkovnimi nizi določa:

„V primeru podatkovnega niza, ki vsebuje osebne in neosebne podatke, se ta uredba uporablja za del podatkovnega niza, ki obsega neosebne podatke. Kadar so osebni in neosebni podatki v podatkovnem nizu neločljivo povezani, ta uredba ne posega v uporabo Uredbe (EU) 2016/679."

To pomeni, da v primeru podatkovnega niza, ki vsebuje osebne in neosebne podatke, velja naslednje:

- uredba o prostem pretoku neosebnih podatkov se uporablja za del podatkovnega niza, ki obsega neosebne podatke;
- določba o prostem pretoku[26] iz splošne uredbe o varstvu podatkov se uporablja za del podatkovnega niza, ki obsega osebne podatke, ter
- če sta del, ki obsega neosebne podatke, in del, ki obsega osebne podatke, „neločljivo povezana", se pravice in obveznosti v zvezi z varstvom podatkov, ki izhajajo iz splošne uredbe o varstvu podatkov, v celoti uporabljajo za celotni mešani podatkovni niz, tudi če osebni podatki predstavljajo samo majhen del podatkovnega niza[27].

Ta razlaga je v skladu s pravico do varstva osebnih podatkov, ki jo zagotavlja Listina Evropske unije o temeljnih pravicah[28], in z uvodno izjavo 8 uredbe o prostem pretoku neosebnih podatkov[29]. Uvodna izjava 8 Uredbe določa, da „[t]a uredba ne vpliva na pravni okvir o varstvu fizičnih oseb glede obdelave osebnih podatkov [...] ter zlasti na [splošno uredbo o varstvu podatkov] in direktivi (EU) 2016/680 in 2002/58/ES [...]".

Praktični primer:

[25] Člen 2(2) Uredbe.

[26] Člen 1(3) 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 (splošna uredba o varstvu podatkov). Glej tudi oddelek 3.2 teh smernic.

[27] Kot je opozorjeno na strani 3 dela 1/2 *delovnega dokumenta služb Komisije o oceni učinka, priloženega predlogu uredbe Evropskega parlamenta in Sveta o okviru za prosti pretok neosebnih podatkov v Evropski uniji* (SWD(2017) 304 final), je treba „ne glede na to, koliko osebnih podatkov je vključenih v mešane podatkovne nize, splošno uredbo o varstvu podatkov v celoti upoštevati v zvezi z delom niza, ki obsega osebne podatke".

[28] Listina Evropske unije o temeljnih pravicah, UL C 362, 26.10.2012, str. 391.

[29] Uvodna izjava 8 Uredbe.

družba, ki deluje v EU, svoje storitve ponuja prek platforme. Podjetja naložijo svoje dokumente, ki vsebujejo mešane podatkovne nize, da lahko uporabljajo njene storitve. Podjetje, ki naloži dokumente, mora kot „upravljavec“ zagotoviti, da je obdelava v skladu s splošno uredbo o varstvu podatkov. Družba, ki ponuja storitve („obdelovalec“), mora z obdelavo podatkovnega niza v imenu upravljavca podatke shraniti in obdelati v skladu s splošno uredbo o varstvu podatkov, da bi na primer zagotovila, da je zajamčena ustrezna raven varnosti v zvezi s podatki, vključno s šifriranjem.

Pojem „neločljivo povezan“ ni opredeljen v nobeni od navedenih uredb[30]. Iz praktičnih razlogov se lahko nanaša na položaj, v katerem podatkovni niz vsebuje osebne in neosebne podatke, pri čemer bi bilo ločevanje teh dveh vrst podatkov nemogoče ali pa bi bilo ločevanje po mnenju upravljavca ekonomsko neučinkovito ali tehnično neizvedljivo. Pri nakupu sistemov za upravljanje odnosov s strankami (CRM) in poročanje o prodaji bi morala družba na primer podvojiti svoje stroške za programsko opremo, saj bi morala kupiti ločeno programsko opremo za CRM (osebni podatki) in sisteme za poročanje o prodaji (zbirni/neosebni podatki) na podlagi podatkov CRM.

Ločevanje podatkovnega niza bi verjetno tudi bistveno zmanjšalo njegovo vrednost. Poleg tega je zaradi spreminjajoče se narave podatkov (glej oddelek 2.1) težje jasno razlikovati med različnimi kategorijami podatkov in jih tako ločiti.

Pomembno je, da nobena od uredb podjetij ne zavezuje k ločevanju podatkovnih nizov, ki jih upravljajo ali obdelujejo.

Zato bodo za mešani podatkovni niz na splošno veljale obveznosti upravljavcev in obdelovalcev podatkov ter zahteve glede spoštovanja pravic posameznikov, na katere se nanašajo osebni podatki, iz splošne uredbe o varstvu podatkov.

Obdelava podatkov o zdravstvenem stanju

Podatki o zdravstvenem stanju so lahko del mešanega podatkovnega niza. Med primeri so elektronski zdravstveni zapisi, klinični preskusi ali nizi podatkov, zbrani z različnimi mobilnimi aplikacijami za zdravje in dobro počutje (kot so aplikacije za merjenje zdravstvenega stanja, za opominjanje, kdaj moramo vzeti zdravila, ali za spremljanje našega napredka glede telesne pripravljenosti)[31]. Zaradi tehnološkega razvoja natančna ločnica med osebnimi in neosebnimi podatki v teh podatkovnih nizih postaja vse bolj nejasna. Zato mora biti njihova obdelava v skladu s splošno uredbo o varstvu podatkov, zlasti (glede na to, da so podatki o zdravstvenem stanju v skladu z Uredbo posebna vrsta podatkov) s členom 9, ki določa splošno prepoved obdelave posebnih vrst podatkov in izjeme od nje.

Podatki v mešanih podatkovnih nizih, ki vsebujejo podatke o zdravstvenem stanju, so lahko dragocen vir informacij, na primer za nadaljnje medicinske raziskave, merjenje stranskih učinkov predpisanega zdravila, statistične namene v zvezi z boleznimi ali razvoj novih zdravstvenih storitev ali zdravljenja. Vendar pa je treba pri izvajanju začetnih dejanj obdelave in nadaljnjih dejanj obdelave podatkov upoštevati splošno uredbo o varstvu podatkov. Zato mora imeti vsaka taka obdelava podatkov o

[30] Uredba o prostem pretoku neosebnih podatkov in splošna uredba o varstvu podatkov.

[31] Za razvoj in delovanje mobilnih aplikacij za zdravje je treba strogo upoštevati pravila splošne uredbe o varstvu podatkov. Te zahteve bodo podrobneje opredeljene v kodeksu ravnanja o zasebnosti za mobilne aplikacije za zdravje, ki se trenutno pripravlja. Več informacij o stanju glede njegove priprave je na voljo na spletnem naslovu: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

zdravstvenem stanju veljavno pravno podlago[32], biti mora ustrezno utemeljena in varna ter zagotavljati zadostne zaščitne ukrepe.

Nazadnje je bistveno, da imajo posamezniki in podjetja pravno varnost ter zaupajo v obdelavo podatkov. To je ključno tudi za podatkovno gospodarstvo. Uredbi to zagotavljata, pri čemer se z njima ne poskuša spremeniti prosti pretok podatkov.

3 Prosti pretok podatkov in odprava zahtev glede lokalizacije podatkov

V tem oddelku so podrobneje pojasnjeni pojmi zahtev glede lokalizacije podatkov iz uredbe o prostem pretoku neosebnih podatkov in načela prostega pretoka iz splošne uredbe o varstvu podatkov. Čeprav so te določbe namenjene državam članicam, so lahko informativne za podjetja, da imajo natančnejšo predstavo o tem, kako ti dve uredbi prispevata k prostemu pretoku vseh podatkov v EU.

3.1 Prosti pretok neosebnih podatkov

Uredba o prostem pretoku neosebnih podatkov[33] določa: „[z]ahteve glede lokalizacije podatkov so prepovedane, razen če so utemeljene na podlagi javne varnosti ob upoštevanju načela sorazmernosti.“

Zahteve glede lokalizacije podatkov so opredeljene[34] kot „kakršn[a] koli obveznost, prepoved, pogoj, omejitev ali drug[a] zahtev[a], ki je določena v zakonih ali drugih predpisih države članice ali izhaja iz splošne in dosledne administrativne prakse v državi članici in osebah javnega prava, vključno s tistimi, povezanimi z javnim naročanjem, brez poseganja v Direktivo 2014/24/EU, in ki določa, da mora obdelava podatkov potekati na ozemlju določene države članice ali omejuje obdelavo podatkov v drugi državi članici[35].“

Iz opredelitve je razvidno, da imajo lahko ukrepi, ki omejujejo prosti pretok podatkov v EU, različne oblike. Določeni so lahko z zakoni, upravnimi predpisi in določbami ali celo izhajajo iz splošnih in doslednih upravnih praks. Poleg tega prepoved zahtev glede lokalizacije podatkov zajema neposredne in posredne ukrepe, ki bi omejili prosti pretok neosebnih podatkov.

Neposredne zahteve glede lokalizacije podatkov lahko obsegajo na primer obveznost shranjevanja podatkov na določeni geografski lokaciji (npr. strežniki morajo biti v določeni državi članici) ali obveznost izpolnjevanja enotnih nacionalnih tehničnih zahtev (npr. podatki morajo biti v posebnih nacionalnih formatih).

Posredne zahteve glede lokalizacije podatkov, ki bi v vseh drugih državah članicah ovirale obdelavo neosebnih podatkov, so lahko v različnih oblikah. Vključujejo lahko zahteve za uporabo tehnoloških

[32] Glej člen 6(1) 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 (splošna uredba o varstvu podatkov).

[33] Člen 4(1) Uredbe.

[34] Člen 3(5) Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[35] Opozoriti je treba, da pravna negotovost pri obsegu zakonitih in nezakonitih zahtev glede lokalizacije podatkov dodatno omejuje možnosti izbire v zvezi z lokacijo obdelave podatkov, ki so na voljo subjektom na trgu in javnemu sektorju (glej uvodno izjavo 4 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji).

naprav, certificiranih ali odobrenih v določeni državi članici, ali druge zahteve, katerih učinek je, da otežujejo obdelavo podatkov zunaj določenega geografskega območja ali ozemlja v Evropski uniji[36,37].

Pri oceni, ali določen ukrep predstavlja posredno zahtevo glede lokalizacije podatkov, je treba upoštevati posebne okoliščine posameznega primera.

V uredbi o prostem pretoku neosebnih podatkov[38] je naveden pojem **javna varnost**, kot je opisan v sodni praksi Sodišča Evropske unije. Javna varnost „zajema tako notranjo kot zunanjo varnost države članice[39] ter vprašanja varnosti ljudi, zlasti za olajšanje preiskovanja, odkrivanja in pregona kaznivih dejanj. Predpostavlja obstoj dejanske in dovolj resne grožnje, ki vpliva na enega od temeljnih interesov družbe[40], kot je ogrožanje delovanja institucij in temeljnih javnih služb ter preživetja prebivalstva, pa tudi tveganje resnih motenj v zunanjih odnosih ali v mirnem sobivanju narodov oziroma grožnjo vojaškim interesom.“

Poleg tega morajo biti vse zahteve glede lokalizacije podatkov, upravičene iz razlogov javne varnosti, sorazmerne. V skladu s sodno prakso Sodišča Evropske unije načelo sorazmernosti nalaga, da so sprejeti ukrepi primerni za uresničitev zastavljenega cilja in ne presegajo tistega, kar je potrebno za navedeni namen[41].

Zaradi jasnosti prepoved zahtev glede lokalizacije podatkov ne posega v že obstoječe omejitve, ki jih določa pravo EU[42].

Poleg tega uredba o prostem pretoku neosebnih podatkov podjetjem ne nalaga nobenih obveznosti in ne omejuje njihove pogodbene svobode pri odločanju, kje bodo obdelani njihovi podatki.

---

[36] Uvodna izjava 4 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[37] Glej študiji o zahtevah glede lokalizacije podatkov, ki sta bili izvedeni pred sprejetjem uredbe o prostem pretoku neosebnih podatkov: (1) Godel, M., idr.: *Facilitating cross border data flows in the Digital Single Market* (Olajševanje čezmejnih tokov podatkov na enotnem digitalnem trgu), številka SMART 2015/2016. Na voljo na spletnem naslovu: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185; ter (2) Time.lex, Spark Legal Network in Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions (Čezmejni pretok podatkov na enotnem digitalnem trgu: študija o omejitvah za lokalizacijo podatkov)*, številka SMART 2015/0054. Na voljo na spletnem naslovu: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695.

[38] Uvodna izjava 19 Uredbe.

[39] Glej na primer sodbo Sodišča z dne 23. novembra 2010, *Land Baden-Württemberg* proti *Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, točka 43, in sodbo z dne 4. aprila 2017, *Sahar Fahimian* proti *Zvezni republiki Nemčiji*, C-544/15, ECLI:EU:C:2017:225, točka 39.

[40] Glej na primer sodbo Sodišča z dne 22. decembra 2008, *Komisija Evropskih skupnosti* proti *Republiki Avstriji*, C-161/07, ECLI:EU:C:2008:759, točka 35, in v njej navedeno sodno prakso ter sodbo z dne 26. marca 2009, *Komisija Evropskih skupnosti* proti *Italijanski republiki*, C-326/07, ECLI:EC:C:2009:193, točka 70, in v njej navedeno sodno prakso.

[41] Glej na primer sodbo Sodišča z dne 8. julija 2010, *Afton Chemical Limited* proti *Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, točka 45, in tudi v njej navedeno sodno prakso.

[42] Glej na primer člen 245(2) Direktive 2006/112/ES z dne 28. novembra 2006 o skupnem sistemu davka na dodano vrednost, ki določa: „Države članice lahko od davčnih zavezancev s sedežem na njihovem ozemlju zahtevajo, da jih obvestijo o kraju hrambe, če je hramba zunaj njihovega ozemlja.“ Vendar je treba to zahtevo brati v skladu s členom 249, v katerem je navedeno: „Ko davčni zavezanec shranjuje račune, ki jih izdaja ali prejema z elektronskimi sredstvi, ki jamči on–line dostop do podatkov[,] in ko je mesto shranjevanja v državi članici, ki ni država članica, v kateri ima sedež, imajo pristojni organi v državi članici, v kateri ima sedež, za namene te direktive pravico dostopa do teh računov z elektronskimi sredstvi, do njihovega prenosa in uporabe v mejah, ki so določene v predpisih države članice, kjer ima davčni zavezanec sedež[,] in kolikor ti organi to zahtevajo za namene nadzora.“

Države članice morajo podrobnosti o vseh zahtevah glede lokalizacije podatkov, ki se uporabljajo na njihovem ozemlju, objaviti na nacionalni enotni spletni informacijski točki (nacionalna spletišča). Te informacije morajo posodabljati ali posodobljene informacije posredovati centralni informacijski točki, ki jo vzpostavlja drug akt EU[43]. Zaradi praktičnosti za podjetja in za olajšanje njihovega dostopa do ustreznih informacij po vsej EU bo Komisija na portalu Tvoja Evropa[44] objavila povezave do teh informacijskih točk.

3.2 Prosti pretok osebnih podatkov

Splošna uredba o varstvu podatkov[45] določa, da „[p]rosti pretok osebnih podatkov v Uniji ne sme biti omejen ali prepovedan iz razlogov, povezanih z varstvom posameznikov pri obdelavi osebnih podatkov."

Če država članica iz razlogov, ki niso varstvo osebnih podatkov, uvede zahteve glede lokalizacije osebnih podatkov, bodo morale biti te zahteve ocenjene glede na določbe o temeljnih svoboščinah in dovoljenih razlogih za odstopanje od teh svoboščin v Pogodbi o delovanju Evropske unije[46,47] ter ustrezni zakonodaji EU, kot sta direktiva o storitvah[48] in direktiva o e-poslovanju[49].

Primer:

nacionalni zakon iz razlogov, povezanih z regulativnim nadzorom, na primer s strani nacionalnega davčnega organa, zahteva, da so računi za izplačevanje plač odprti v določeni državi članici. Taka nacionalna določba ne bi spadala v področje uporabe člena 1(3) splošne uredbe o varstvu podatkov, ker razlogi zanjo niso varstvo osebnih podatkov. Namesto tega bi bilo treba to zahtevo oceniti glede na določbe o temeljnih svoboščinah in dovoljenih razlogih za odstopanje od teh svoboščin v Pogodbi o delovanju Evropske unije.

V Splošni uredbi o varstvu podatkov[50] je priznano, da lahko države članice uvedejo pogoje, tudi omejitve, glede obdelave genetskih podatkov, biometričnih podatkov ali podatkov o zdravstvenem stanju. Kot je navedeno v uvodni izjavi 53, pa takšne nacionalne omejitve ne bi smele ovirati prostega pretoka osebnih podatkov v EU, kadar ti pogoji veljajo za čezmejno obdelavo takih podatkov. To je v

[43] Člen 4(4) Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[44] https://europa.eu/youreurope/index.htm

[45] Člen 1(3) 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 (splošna uredba o varstvu podatkov).

[46] Prečiščena različica Pogodbe o delovanju Evropske unije, UL C 326, 26.10.2012, str. 47.

[47] Glej tudi sodbo Sodišča z dne 19. junija 2008, *Komisija Evropskih skupnosti* proti *Velikemu vojvodstvu Luksemburg*, C-319/06, ECLI:EU:C:2008:350, točki 90 in 91: Sodišče je menilo, da obveznost priprave in hrambe določenih dokumentov v določeni državi članici pomeni omejitev svobode opravljanja storitev; utemeljitev, da bi taka hramba „organom [...] na splošno olajšal[a] izpolnitev naloge nadzora", ne zadostuje.

[48] Direktiva 2006/123/ES Evropskega parlamenta in Sveta z dne 12. decembra 2006 o storitvah na notranjem trgu, UL L 376, 27.12.2006, str. 36.

[49] Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju), UL L 178, 17.7.2000, str. 1.

[50] Člen 9(4) 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 (splošna uredba o varstvu podatkov).

skladu s členom 16 Pogodbe o delovanju Evropske unije, ki zagotavlja pravno podlago za sprejetje pravil o pravici do varstva osebnih podatkov in prostem pretoku takih podatkov.

3.3 Področje uporabe uredbe o prostem pretoku neosebnih podatkov

Kot je bilo že navedeno, je cilj uredbe o prostem pretoku neosebnih podatkov zagotoviti prosti pretok neosebnih podatkov „v Uniji“[51]. Zato se Uredba ne uporablja za dejanja obdelave, ki potekajo zunaj EU, in za zahteve glede lokalizacije podatkov, ki zadevajo to obdelavo[52,53].

Zato je področje uporabe Uredbe v skladu s členom 2(1) omejeno na obdelavo elektronskih neosebnih podatkov v EU, ki:

(a) se opravlja kot storitev za uporabnike, ki prebivajo ali imajo sedež v EU, ne glede na to, ali ima ponudnik storitev sedež v EU ali ne, ali
(b) jo za lastne potrebe izvaja fizična ali pravna oseba, ki prebiva ali ima sedež v EU.

Primeri:

člen 2(1)(a) uredbe o prostem pretoku neosebnih podatkov:

- ponudnik storitev v oblaku s sedežem v ZDA zagotavlja storitve obdelave strankam, ki prebivajo ali imajo sedež v EU. Svoje dejavnosti upravlja prek strežnikov na ozemlju EU, kjer so shranjeni ali drugače obdelani podatki njegovih evropskih strank. Ponudniku storitev v oblaku ni treba biti lastnik infrastrukture v EU, saj lahko na primer najame strežniški prostor v EU. Uredba o prostem pretoku neosebnih podatkov se uporablja za tako obdelavo podatkov.
- Ponudnik storitev v oblaku s sedežem na Japonskem ponuja svoje storitve evropskim strankam. Sistemi ponudnika za obdelavo podatkov se nahajajo na Japonskem, kjer potekajo vse dejavnosti obdelave. Uredba o prostem pretoku neosebnih podatkov se v tem primeru ne uporablja, če vse dejavnosti obdelave potekajo zunaj EU[54].

Člen 2(1)(b) uredbe o prostem pretoku neosebnih podatkov:

- majhno evropsko zagonsko podjetje iz države članice A se odloči, da bo z odprtjem poslovne enote v državi članici B povečalo obseg svojega poslovanja. Da bi čim bolj znižalo stroške, se odloči centralizirati shranjevanje in obdelavo podatkov nove poslovne enote na svojem

[51] Glej člen 1 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.
[52] Glej uvodno izjavo 15 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.
[53] Pojem „obdelava“ je opredeljen v širšem smislu (člen 3(2) Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji), v uvodni izjavi 17 pa je poudarjeno, da bi se morala Uredba uporabljati za obdelavo v najširšem smislu in vključevati uporabo vseh vrst informacijskih sistemov.
[54] Opozoriti je treba, da se Uredba (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji ne nanaša na zahteve glede lokalizacije podatkov, ki jih države članice uvedejo za hrambo neosebnih podatkov v tretjih državah, zato so lahko take zahteve prisotne v nacionalnih pravnih redih. Zaradi jasnosti se splošna uredba o varstvu podatkov uporablja za obdelavo osebnih podatkov posameznikov, na katere se nanašajo osebni podatki in ki so v EU, s strani upravljavca ali obdelovalca, ki nima sedeža v EU, kadar so dejavnosti obdelave povezane: (a) z nudenjem blaga ali storitev takim posameznikom v Uniji, ne glede na to, ali je potrebno plačilo posameznika, na katerega se nanašajo osebni podatki, ali (b) s spremljanjem njihovega vedenja, kolikor to poteka v Uniji (glej člen 3(2) Splošne uredbe o varstvu podatkov).

strežniku, ki je v državi članici A. Države članice ne smejo prepovedati takih prizadevanj za centralizacijo informacijske tehnologije, razen če je to utemeljeno na podlagi javne varnosti ob upoštevanju načela sorazmernosti.

Čeprav se uredba o prostem pretoku neosebnih podatkov ne uporablja, če se vse dejavnosti obdelave neosebnih podatkov izvajajo zunaj EU, je treba upoštevati splošno uredbo o varstvu podatkov, kadar podatkovni niz vsebuje osebne podatke. Zlasti je treba vsekakor upoštevati pravila za prenos osebnih podatkov v tretje države ali mednarodne organizacije v skladu s splošno uredbo o varstvu podatkov[55].

3.4 Dejavnosti v zvezi z notranjo organizacijo držav članic

Uredba o prostem pretoku neosebnih podatkov držav članic ne obvezuje, da na zunanje izvajalce prenesejo opravljanje storitev v zvezi z neosebnimi podatki, ki jih želijo opravljati sami ali jih organizirati na drug način kot pa z javnimi naročili[56].

V drugem pododstavku člena 2(3) uredbe o prostem pretoku neosebnih podatkov je navedeno:

„Ta uredba ne posega v zakone in druge predpise v zvezi z **notranjo organizacijo** držav članic, ki določajo prenos pristojnosti in pooblastil za **obdelavo podatkov brez pogodbenih plačil zasebnih strank** na javne organe in osebe javnega prava, kakor so opredeljene v točki (4) člena 2(1) Direktive 2014/24/EU[57], kot tudi ne v zakone in druge predpise držav članic, ki določajo izvajanje teh pooblastil in pristojnosti.“[58]

Obstajajo lahko legitimni interesi, ki bi upravičili izbiro tovrstnega „samozagotavljanja“ storitev obdelave podatkov, kot so „notranje izvajanje“ ali medsebojni dogovori med javnimi upravami. Značilni primeri vključujejo uporabo „vladnega oblaka“ ali vlado, ki za zagotavljanje storitev obdelave podatkov za javne institucije in organe najame centralizirano agencijo za informacijsko tehnologijo.

[55] V zvezi s prenosi osebnih podatkov v tretje države glej spletno stran Komisije: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_sl in *Sporočilo Komisije Evropskemu parlamentu in Svetu – Izmenjava in varstvo osebnih podatkov v globaliziranem svetu*, COM(2017) 7 final, ki je na voljo na spletnem naslovu: https://eur-lex.europa.eu/legal-content/SL/TXT/?qid=1557829767202&uri=CELEX:52017DC0007. Komisija je v zvezi z Japonsko 23. januarja 2019 sprejela sklep o ustreznosti, ki omogoča prosti pretok osebnih podatkov med gospodarstvoma na podlagi jamstev o visoki ravni varstva teh podatkov.

[56] Uvodna izjava 14 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[57] Člen 2(1)(4) Direktive 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES, UL L 94, 28.3.2014, str. 65, določa, da „osebe javnega prava“ pomenijo osebe, ki imajo vse naslednje značilnosti: (a) ustanovljene so s posebnim namenom, da zadovoljujejo potrebe splošnega interesa, ki niso industrijske ali poslovne narave; (b) so pravne osebe in (c) jih večinoma financirajo državni, regionalni ali lokalni organi ali druge osebe javnega prava ali so pod upravljavskim nadzorom teh organov ali oseb ali imajo upravni, vodstveni ali nadzorni organ, v katerega več kot polovico članov imenujejo državni, regionalni ali lokalni organi ali druge osebe javnega prava;“

[58] V uvodni izjavi 13 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji je poudarjeno, da Uredba ne posega v Direktivo 2014/24/EU.

Vendar pa uredba o prostem pretoku neosebnih podatkov države članice spodbuja, naj preučijo gospodarsko učinkovitost in druge prednosti uporabe zunanjih ponudnikov storitev[59],[60]. Takoj ko začnejo nacionalni organi obdelavo podatkov oddajati v „zunanje izvajanje“ s pogodbenim plačilom zasebnim subjektom in se obdelava izvaja v EU, zanjo velja uredba o prostem pretoku neosebnih podatkov, kar pomeni, da se načelo prostega pretoka neosebnih podatkov uporablja za splošne in administrativne prakse nacionalnih organov. Zlasti se morajo vzdržati določanja omejitev za lokalizacijo podatkov, na primer v javnih razpisih[61]..

4 Samoregulativni pristopi, ki podpirajo prosti pretok podatkov

Samoregulacija prispeva k inovacijam in zaupanju med subjekti na trgu ter se lahko bolje odziva na spremembe na trgu. Ta oddelek vsebuje pregled samoregulativnih pobud za obdelavo osebnih in neosebnih podatkov.

4.1 Prenos podatkov in zamenjava ponudnikov storitev v oblaku

Eden od namenov uredbe o prostem pretoku neosebnih podatkov je preprečevanje praks, ki povzročajo vezanost na ponudnika. Te prakse se pojavijo, kadar uporabniki ne morejo zamenjati ponudnika storitev, ker so njihovi podatki „zaklenjeni“ v sistemu ponudnika, na primer zaradi posebnega formata podatkov ali pogodbenih dogovorov, in jih ni mogoče prenesti iz informacijskega sistema ponudnika. Neoviran prenos podatkov je pomemben, da lahko uporabniki svobodno izbirajo med ponudniki storitev obdelave podatkov in da se tako zagotovi učinkovita konkurenca na trgu.

Prenosljivost podatkov med podjetji postaja vse pomembnejša v številnih digitalnih panogah, vključno s storitvami v oblaku.

V skladu s členom 6 uredbe o prostem pretoku neosebnih podatkov Komisija spodbuja in olajšuje pripravo samoregulativnih kodeksov ravnanja na ravni EU (v nadaljnjem besedilu: kodeksi ravnanja), da se prispeva h konkurenčnemu podatkovnemu gospodarstvu. Industriji zagotavlja podlago za pripravo samoregulativnih kodeksov ravnanja o zamenjavi ponudnikov storitev in prenosu podatkov med različnimi informacijskimi sistemi.

Pri pripravi takih kodeksov ravnanja o prenosu podatkov je treba upoštevati več vidikov, zlasti:

- dobre prakse za lažjo zamenjavo ponudnika storitev in lažji prenos podatkov v strukturirani, splošno uporabljani in strojno berljivi obliki;
- **zahteve za minimalne informacije**, da se poklicnim uporabnikom pred sklenitvijo pogodbe zagotovijo dovolj podrobne in jasne informacije v zvezi s postopki, tehničnimi zahtevami, roki in stroški, ki se uporabljajo v primeru, da poklicni uporabnik želi zamenjati ponudnika storitev ali prenesti podatke nazaj v lastne informacijske sisteme;
- **pristope k certifikacijskim shemam** za boljšo primerljivost storitev v oblaku ter
- komunikacijske načrte za ozaveščanje o kodeksih ravnanja.

[59] Uvodna izjava 14 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[60] Zunanji ponudnik storitev bi bil vsak subjekt, ki ni „oseba javnega prava“, kot je določena v členu 2(1)(4) Direktive 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES, UL L 94, 28.3.2014, str. 65.

[61] Uvodna izjava 13 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

Komisija je na trgu storitev v oblaku začela spodbujati delo delovnih skupin deležnikov na področju storitev v oblaku na digitalnem enotnem trgu, ki združujejo strokovnjake na področju storitev v oblaku in poklicne uporabnike, vključno z malimi in srednjimi podjetji. V tej fazi ena podskupina pripravlja samoregulativne kodekse ravnanja o prenosu podatkov in zamenjavi ponudnikov storitev v oblaku (delovna skupina SWIPO)[62], druga podskupina pa se ukvarja z razvojem certificiranja varnosti storitev v oblaku (delovna skupina CSPCERT)[63]..

Delovna skupina SWIPO pripravlja kodekse ravnanja, ki zajemajo celotni spekter storitev v oblaku; infrastrukturo kot storitev (Infrastructure as a Service – IaaS), platformo kot storitev (Platform as a service – PaaS) in programsko opremo kot storitev (Software as a service – SaaS).

Komisija pričakuje, da bodo različni kodeksi ravnanja dopolnjeni z vzorčnimi pogodbenimi klavzulami[64]. Te bodo omogočile zadostno tehnično in pravno specifičnost pri praktičnem izvajanju in uporabi kodeksov ravnanja, kar bo posebej pomembno za mala in srednja podjetja. Načrtuje se, da bodo vzorčne pogodbene klavzule oblikovane po pripravi kodeksov ravnanja (ki naj bi bili pripravljeni do 29. novembra 2019).

Komisija bo v skladu s členom 8 uredbe o prostem pretoku neosebnih podatkov do 29. novembra 2022 ocenila izvajanje Uredbe. Tako bo mogoče oceniti: (i) vpliv na prosti pretok podatkov v Evropi; (ii) uporabo Uredbe, zlasti za mešane podatkovne nize; (iii) koliko so države članice dejansko odpravile obstoječe neupravičene omejitve za lokalizacijo podatkov ter (iv) tržno učinkovitost kodeksov ravnanja na področju prenosa podatkov in zamenjave ponudnikov storitev v oblaku.

Pojem prenosljivosti in medsebojno vplivanje s splošno uredbo o varstvu podatkov

Obe uredbi[65] se nanašata na prenosljivost podatkov in cilj olajšati prenos podatkov iz enega informacijskega okolja v drugega, tj. v sisteme drugega ponudnika ali sisteme na kraju samem. To preprečuje vezanost na ponudnika in spodbuja konkurenco med ponudniki storitev. Vendar pa se uredbi razlikujeta po pristopu k prenosljivosti, kadar gre za odnos med ciljnimi interesnimi skupinami in pravno naravo določb.

Pravica do prenosljivosti podatkov iz člena 20 splošne uredbe o varstvu podatkov zadeva zlasti odnos med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem. To je pravica posameznika, na katerega se nanašajo osebni podatki, da prejme osebne podatke, ki jih je posedoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, ter da te podatke posreduje drugemu upravljavcu ali jih prenese v lastni sistem za hrambo podatkov, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral[66]. V tem odnosu so posamezniki, na katere se

[62] *Cloud Switching and Porting Data Working Group* (delovna skupina za zamenjavo ponudnikov storitev v oblaku in prenos podatkov).

[63] *European Cloud Service Provider Certification Working Group* (delovna skupina za certificiranje evropskih ponudnikov storitev v oblaku). Glej tudi oddelek 4.3.

[64] Glej uvodno izjavo 30 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji.

[65] Člen 6 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji ter člen 20 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 (splošna uredba o varstvu podatkov).

[66] Glej mnenje delovne skupine iz člena 29: Smernice o pravici do prenosljivosti podatkov, WP 242 rev. 01, sprejete 13. decembra 2016, kot so bile nazadnje revidirane in sprejete 5. aprila 2017.

nanašajo osebni podatki, običajno potrošniki različnih spletnih storitev, ki želijo zamenjati te ponudnike storitev.

Člen 6 uredbe o prostem pretoku neosebnih podatkov ne določa pravice poklicnih uporabnikov do prenosa podatkov, ampak vsebuje samoregulativni pristop s prostovoljnimi kodeksi ravnanja za industrijo. Hkrati je usmerjen v položaj, v katerem je poklicni uporabnik obdelavo podatkov oddal v zunanje izvajanje tretji osebi, ki ponuja storitev obdelave podatkov[67]. V skladu s členom 3(8) uredbe o prostem pretoku neosebnih podatkov lahko pojem „poklicni uporabnik“ zajema „fizično ali pravno osebo, vključno z javnim organom ali osebo javnega prava, ki uporablja ali naroči storitev obdelave podatkov za namene v zvezi s svojo trgovsko, poslovno, obrtno ali poklicno dejavnostjo oziroma izpolnjevanjem nalog“.

V praksi prenosljivost v skladu s členom 6 uredbe o prostem pretoku neosebnih podatkov zadeva interakcije med podjetji, in sicer med poklicnim uporabnikom (ki se lahko v primerih, ki vključujejo obdelavo osebnih podatkov, v skladu s splošno uredbo o varstvu podatkov šteje za „upravljavca“) in ponudnikom storitev (ki ga je treba v nekaterih primerih podobno šteti za „obdelovalca“).

Kljub razlikam se lahko pojavijo primeri, v katerih bi za prenos podatkov v zvezi z mešanimi podatkovnimi nizi veljala tako uredba o prostem pretoku neosebnih podatkov kot tudi splošna uredba o varstvu podatkov.

Primer:

podjetje, ki uporablja storitev v oblaku, se odloči za zamenjavo ponudnika storitev v oblaku in prenos vseh podatkov na novega ponudnika. Zamenjava ponudnika storitev in prenos podatkov sta zajeta v pogodbi med stranko in ponudnikom storitev v oblaku. Če stari ponudnik storitev v oblaku upošteva kodekse ravnanja, pripravljene v skladu z uredbo o prostem pretoku neosebnih podatkov, je treba podatke prenesti v skladu z zahtevami, določenimi v navedenih kodeksih.

Če preneseni podatkovni nizi vsebujejo tudi osebne podatke, mora biti prenos v skladu z vsemi ustreznimi določbami splošne uredbe o varstvu podatkov, pri čemer je treba zlasti zagotoviti, da novi ponudnik storitev v oblaku izpolnjuje veljavne zahteve, na primer glede varnosti[68].

Primer:

če se banka odloči za zamenjavo svojega ponudnika storitev upravljanja odnosov s strankami, je možno, da je treba nekatere (osebne in neosebne) podatke prenesti s starega ponudnika na novega. Za te podatke bodo nato veljale različne regulativne zahteve, pri čemer nekatere izhajajo iz splošne uredbe o varstvu podatkov, druge pa iz uredbe o prostem pretoku neosebnih podatkov.

[67] V uvodni izjavi 29 Uredbe (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji je navedeno: „Medtem ko potrošnikom posameznikom obstoječe pravo Unije [tj. splošna uredba o varstvu podatkov] koristi, pa uporabnikom, ki izvajajo poslovne ali poklicne dejavnosti, ni olajšana možnost zamenjave ponudnika storitev.“

[68] Glej mnenje delovne skupine iz člena 29: Mnenje št. 5/2012 o računalništvu v oblaku, sprejeto 1. julija 2012, WP196, v katerem so podrobneje določeni položaj in obveznosti uporabnikov in ponudnikov storitev v oblaku v zvezi z obdelavo osebnih podatkov.

4.2 Kodeksi ravnanja in certifikacijske sheme v zvezi z varstvom osebnih podatkov

Izpolnjevanje obveznosti iz Splošne uredbe o varstvu podatkov se lahko dokaže s kodeksi ravnanja in certifikacijskimi shemami (glej člen 24(3) in člen 28(5)).

V skladu s členom 40(1) in členom 42(1) Splošne uredbe o varstvu podatkov bi morali države članice, nadzorni organi, Evropski odbor za varstvo podatkov in Komisija industrijo spodbujati, naj pripravi kodekse ravnanja in vzpostavi mehanizme certificiranja za varstvo podatkov.

Združenja ali drugi organi, ki predstavljajo posebno kategorijo upravljavcev ali obdelovalcev, lahko pripravijo kodeks ravnanja za določen sektor. Osnutek kodeksa je treba predložiti v odobritev zadevnemu pristojnemu nadzornemu organu[69]. Če se osnutek kodeksa ravnanja nanaša na dejavnosti obdelave v več državah članicah, ga mora nadzorni organ pred odobritvijo predložiti Evropskemu odboru za varstvo podatkov. Odbor bo nato predložil mnenje, ali je osnutek kodeksa skladen s Splošno uredbo o varstvu podatkov.

Evropski odbor za varstvo podatkov je objavil Smernice št. 1/2019 o kodeksih ravnanja in organih za spremljanje na podlagi Splošne uredbe o varstvu podatkov[70]. Smernice vsebujejo informacije o pripravi kodeksov ravnanja in merilih za njihovo odobritev ter druge koristne informacije. Smernice Evropskega odbora za varstvo podatkov št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Splošne uredbe o varstvu podatkov prav tako zagotavljajo informacije o certificiranju na podlagi navedene uredbe ter o oblikovanju in odobritvi meril za certificiranje[71].

Primeri kodeksov ravnanja, pripravljenih v okviru industrije storitev v oblaku:

Kodeks ravnanja EU za storitve v oblaku, katerega pripravo je omogočila Komisija, je bil pripravljen v sodelovanju s skupino Cloud Select Industry Group (C-SIG) na podlagi direktive o varstvu podatkov[72], pozneje pa na podlagi Splošne uredbe o varstvu podatkov. Zajema celotni spekter storitev v oblaku – programsko opremo kot storitev (SaaS), platformo kot storitev (PaaS) in infrastrukturo kot storitev (IaaS)[73].

Kodeks ravnanja ponudnikov infrastrukturnih storitev v oblaku v Evropi (*Cloud Infrastructure Services Providers in Europe* – CISPE)[74] je osredotočen na ponudnike storitev IaaS. Kodeks ravnanja

[69] Glej člen 40(5) in člen 55 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 (Splošna uredba o varstvu podatkov).

[70] Evropski odbor za varstvo podatkov: *Smernice št. 1/2019 o kodeksih ravnanja in organih za spremljanje na podlagi Uredbe 2016/679*, sprejete 12. februarja 2019, različica za javno posvetovanje, na voljo na spletnem naslovu: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_sl.

[71] Evropski odbor za varstvo podatkov: *Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe (EU) 2016/679*, sprejete 23. januarja 2019, na voljo na spletnem naslovu: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_sl.

[72] 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 (datum izteka veljavnosti: 24. maj 2018).

[73] Več informacij o kodeksu ravnanja EU za storitve v oblaku je na voljo na spletnem naslovu: https://eucoc.cloud/en/home.html.

[74] Več informacij o kodeksu ravnanja CISPE je na voljo na spletnem naslovu: https://cispe.cloud/code-of-conduct/.

CISPE vsebuje zahteve, ki se nanašajo na ponudnike storitev IaaS, ki delujejo kot obdelovalci podatkov v skladu s Splošno uredbo o varstvu podatkov. Določa tudi določbe o strukturi upravljanja za izvajanje in uporabo kodeksa.

Kodeks ravnanja zveze *Cloud Security Alliance* (CSA) za skladnost s splošno uredbo o varstvu podatkov je namenjen vsem zainteresiranim deležnikom na področju računalništva v oblaku in evropske zakonodaje o osebnih podatkih, kot so ponudniki in uporabniki storitev v oblaku ter potencialne stranke, revizorji storitev v oblaku in posredniki do ponudnikov storitev v oblaku. Kodeks ravnanja zajema celotni spekter ponudnikov storitev v oblaku[75].

4.3 Spodbujanje zaupanja v čezmejno obdelavo podatkov – certificiranje varnosti

Kot je navedeno v uvodni izjavi 33 uredbe o prostem pretoku neosebnih podatkov, bi se morala s spodbujanjem zaupanja v varnost čezmejne obdelave podatkov zmanjšati nagnjenost subjektov na trgu in javnega sektorja k uporabi lokalizacije podatkov kot nadomestka za varnost podatkov. Poleg svežnja o kibernetski varnosti, ki ga je Komisija predlagala leta 2017[76], delovna skupina CSPCERT pripravlja priporočila za namene vzpostavitve evropske certifikacijske sheme za storitve v oblaku, ki bodo predložena Komisiji. Taka shema lahko olajša prosti pretok podatkov, omogoči boljšo primerljivost storitev v oblaku in spodbuja uporabo storitev v oblaku. Komisija lahko Agencijo Evropske unije za kibernetsko varnost (ENISA) zaprosi, naj v skladu z ustreznimi določbami akta o kibernetski varnosti[77] pripravi predlog za shemo. V okviru take sheme se lahko obravnavajo osebni in neosebni podatki. Kot je poudarjeno v oddelku 4.2, se lahko za dokazovanje obstoja ustreznih zaščitnih ukrepov za varnost podatkov poleg akta o kibernetski varnosti uporablja tudi splošna uredba o varstvu podatkov[78].

Končne pripombe

Zagotavljanje pravne varnosti in zaupanja v obdelavo podatkov je bistveno za zmožnost EU, da čim bolj izkoristi podatke, kjer se lahko vrednostne verige razvijejo v vseh sektorjih in prek meja. Obe uredbi to zagotavljata in uresničujeta cilj prostega pretoka podatkov. Uredba o prostem pretoku neosebnih podatkov in splošna uredba o varstvu podatkov skupaj gradita temelj za prosti pretok vseh podatkov v Evropski uniji in zelo konkurenčno evropsko podatkovno gospodarstvo.

[75] Več informacij o kodeksu ravnanja CSA je na voljo na spletnem naslovu: https://gdpr.cloudsecurityalliance.org/.

[76] Več informacij je na voljo na spletnem naslovu: https://ec.europa.eu/digital-single-market/en/cyber-security.

[77] Uredba Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (akt o kibernetski varnosti).

[78] Glej uvodno izjavo 74 akta o kibernetski varnosti.