EUROPSKA
KOMISIJA

Bruxelles, 29.5.2019.
COM(2019) 250 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

Smjernice o Uredbi o okviru za slobodan protok neosobnih podataka u Europskoj uniji

Sadržaj

1. Uvod ... 2

Svrha ovih Smjernica ... 3

2. Interakcija između Uredbe o slobodnom protoku neosobnih podataka i Opće uredbe o zaštiti podataka u odnosu na miješane skupove podataka ... 4

2.1. Pojam neosobnih podataka iz Uredbe o slobodnom protoku neosobnih podataka ... 4

Osobni podaci ... 4

Neosobni podaci ... 5

2.2. Miješani skupovi podataka ... 7

3. Slobodan protok podataka i uklanjanje zahtjeva u pogledu lokalizacije podataka ... 11

3.1. Slobodan protok neosobnih podataka ... 11

3.2. Slobodan protok neosobnih podataka ... 13

3.3. Područje primjene Uredbe o slobodnom protoku neosobnih podataka ... 14

3.4. Aktivnosti koje se odnose na unutarnju organizaciju država članica ... 15

4. Samoregulatorni pristupi kojima se podržava slobodan protok podataka ... 16

4.1. Prijenos podataka i promjena pružatelja usluga u oblaku ... 16

Pojam prenosivosti podataka i interakcija s Općom uredbom o zaštiti podataka ... 18

4.2. Kodeksi ponašanja i programi certifikacije u području zaštite osobnih podataka ... 19

4.3. Jačanje povjerenja u prekograničnu obradu podataka – certificiranje sigurnosti ... 21

Završne napomene ... 21

Službe Europske komisije ovaj dokument stavljaju na raspolaganje isključivo u informativne svrhe. Dokument ne sadržava mjerodavno tumačenje Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji i ne predstavlja odluku ili stajalište Europske komisije. Njime se ne dovode u pitanje takve odluke ili stajalište Europske komisije i ovlasti Suda Europske unije u pogledu tumačenja te uredbe u skladu s Ugovorima EU-a.

1. Uvod

U gospodarstvu koje se sve više temelji na podacima protok podataka u središtu je poslovnih procesa poduzeća bez obzira na njihovu veličinu ili sektor. Nove digitalne tehnologije pružaju nove mogućnosti široj javnosti, poduzećima i tijelima javne uprave u Europskoj uniji („EU”).

Kako bi se dodatno povećala prekogranična razmjena podataka i ojačalo podatkovno gospodarstvo, na temelju prijedloga Europske komisije („Komisija”) Europski parlament i Vijeće donijeli su u studenome 2018. Uredbu (EU) 2018/1807 o okviru za slobodan protok neosobnih podataka u Europskoj uniji[1] („Uredba o slobodnom protoku neosobnih podataka”). Uredba se primjenjuje od 28. svibnja 2019. Načelo slobodnog kretanja osobnih podataka već je bilo utvrđeno Uredbom (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ („Opća uredba o zaštiti podataka”)[2]. Sada dakle postoji sveobuhvatan okvir za zajednički europski podatkovni prostor i slobodno kretanje svih podataka u Europskoj uniji[3].

Uredbom o slobodnom protoku neosobnih podataka stvara se pravna sigurnost koja poduzećima omogućuje da svoje podatke obrađuju gdje god to žele u EU-u, povećava se povjerenje u usluge obrade podataka i sprečava ovisnost o određenom pružatelju usluga. Na taj će se način klijentima povećati izbor, poboljšati učinkovitost i potaknuti usvajanje tehnologija u oblaku, a poduzećima u EU-u donijeti znatne uštede. Jedna studija pokazuje da bi poduzeća u EU-u mogla uštedjeti 20-50 % svojih troškova IT-a preseljenjem poslovanja u oblak[4].

Tim dvjema uredbama omogućuje se slobodan protok podataka među državama članicama, a korisnicima usluga obrade podataka upotreba podataka prikupljenih na različitim tržištima EU-a radi poboljšanja njihove produktivnosti i konkurentnosti. Korisnici stoga mogu u potpunosti iskoristiti ekonomije razmjera koje pruža veliko tržište EU-a, poboljšati svoju globalnu konkurentnost i pridonijeti boljoj međusobnoj povezanosti podatkovnog gospodarstva EU-a.

Tri su bitne značajke Uredbe o slobodnom protoku neosobnih podataka:

---

[1] Uredba (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji, SL L 303, 28.11.2018., str. 59.

[2] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), SL L 119, 4.5.2016., str. 1.

[3] Općom uredbom o zaštiti podataka obuhvaćen je i Europski gospodarski prostor (EGP), koji uključuje Island, Lihtenštajn i Norvešku. Osim toga, Uredba o slobodnom protoku neosobnih podataka relevantna je za EGP.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe* (Mjerenje ekonomskog učinka računalstva u oblaku u Europi), SMART 2014/0031, 2016. Dostupno na internetu na: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- državama članicama se u pravilu zabranjuje da uvode zahtjeve u vezi s lokalizacijom podataka. Iznimke od tog pravila mogu se opravdati samo razlozima javne sigurnosti u skladu s načelom proporcionalnosti,
- uspostavlja se mehanizam suradnje kako bi se osiguralo da nadležna tijela i dalje mogu ostvarivati sva propisana prava pristupa podacima koji se obrađuju u drugoj državi članici
- potiče se industrija da, uz potporu Komisije, izradi samoregulatorne kodekse ponašanja koji se odnose na promjenu pružatelja usluga i prijenos podataka.

Svrha ovih Smjernica

Ovim se Smjernicama ispunjavaju odredbe članka 8. stavka 3. Uredbe o slobodnom protoku neosobnih podataka kojima se od Komisije zahtijeva da objavi smjernice o interakciji između te uredbe i Opće uredbe o zaštiti podataka, „posebice u pogledu skupova podataka koji se sastoje od osobnih i neosobnih podataka".

Cilj je ovih Smjernica pomoći korisnicima, posebno malim i srednjim poduzećima, u razumijevanju međusobne povezanosti Uredbe o slobodnom protoku neosobnih podataka i Opće uredbe o zaštiti podataka[5]. U Smjernicama se stoga posebna pozornost posvećuje: i. pojmu neosobnih podataka i osobnih podataka, ii. načelu slobodnog kretanja podataka i zabrani zahtjeva u pogledu lokalizacije podataka na temelju te dvije uredbe i iii. pojmu prenosivosti podataka na temelju Uredbe o slobodnom protoku neosobnih podataka. Smjernicama su obuhvaćeni i samoregulatorni zahtjevi utvrđeni u tim dvjema uredbama.

Uredbom o slobodnom protoku neosobnih podataka obuhvaćeni su samo „podaci koji nisu osobni podaci" kako su definirani u Općoj uredbi o zaštiti podataka. Općom uredbom o zaštiti podataka uređuje se obrada osobnih podataka, što je ključan dio okvira EU-a za zaštitu podataka[6]. Na snagu je u državama članicama stupila 25. svibnja 2018. Tom se uredbom utvrđuju usklađena pravila za zaštitu ljudi u EU-u/EGP-u u vezi s obradom njihovih osobnih podataka i slobodnim kretanjem takvih podataka. Općom uredbom o zaštiti podataka: i. utvrđuje se koje se informacije smatraju osobnim podacima, ii. uspostavlja se pravna osnova za njihovu obradu i iii. među ostalim, utvrđuju se prava i obveze koje treba poštovati pri

[5] Uvodna izjava 37. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

[6]
- Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), SL L 119, 4.5.2016., str. 1.
- Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ, SL L 295, 21.11.2018., str. 39.
- Direktiva (EU) 2016/680 o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, SL L 119, 4.5.2016., str. 89.
- Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), SL L 201, 31.7.2002., str. 37. (trenutačno u postupku revizije).

obradi tih podataka[7]. Kad je riječ o načelu slobodnog kretanja osobnih podataka, člankom 1. stavkom 3. Opće uredbe o zaštiti podataka predviđeno je sljedeće: „Slobodno kretanje osobnih podataka unutar Unije ne ograničava se ni zabranjuje iz razloga povezanih sa zaštitom pojedinaca u pogledu obrade osobnih podataka.”

U većini stvarnih situacija vrlo je vjerojatno da će se skup podataka sastojati od osobnih i neosobnih podataka. Takav se skup podataka često naziva „miješani skup podataka”. U odjeljku 2.2. u nastavku pojašnjava se interakcija između Uredbe o slobodnom protoku neosobnih podataka i Opće uredbe o zaštiti podataka u vezi s miješanim skupovima podataka.

Radi jasnoće potrebno je precizirati da Opća uredba o zaštiti podataka i Uredba o slobodnom protoku neosobnih podataka ne sadržavaju međusobno nespojive obveze.

2. Interakcija između Uredbe o slobodnom protoku neosobnih podataka i Opće uredbe o zaštiti podataka u odnosu na miješane skupove podataka

2.1. Pojam neosobnih podataka iz Uredbe o slobodnom protoku neosobnih podataka

Cilj je Uredbe o slobodnom protoku neosobnih podataka[8] omogućiti slobodan protok podataka koji nisu osobni podaci. U cijelom tekstu Uredbe upotrebljava se pojam „podaci”, koji treba tumačiti kao „podaci koji nisu osobni podaci kako su definirani u članku 4. točki 1. Uredbe (EU) 2016/679 [Opća uredba o zaštiti podataka]”[9]. Takvi podaci, koji se u ovom dokumentu nazivaju i „**neosobnim podacima**”, definiraju se kao suprotnost (*a contrario*) osobnim podacima kako su definirani u Općoj uredbi o zaštiti podataka.

Osobni podaci

U Općoj uredbi o zaštiti podataka navodi se sljedeće: „‚osobni podaci’ znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi (‚ispitanik’); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni

---

[7] Za dodatne smjernice o različitim aspektima Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i zakonodavstva EU-a o zaštiti podataka, vidjeti internetske stranice Europskog odbora za zaštitu podataka, koji je izdao brojne smjernice u skladu s člankom 70. Opće uredbe o zaštiti podataka, na sljedećoj adresi: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en. Na tim stranicama nalaze se i upućivanja na smjernice, preporuke i druge dokumente koje je izdala Radna skupina iz članka 29., prethodnica Europskog odbora za zaštitu podataka. Nadalje, Komisija je radi podizanja svijesti građana i poduzeća o Uredbi (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) izdala komunikaciju o zaštiti podataka sa smjernicama za izravnu primjenu Opće uredbe o zaštiti podataka (COM(2018) 043 final), koja je dostupna na: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

[8] Članak 1. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

[9] Vidjeti članak 3. stavak 1. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca".

Široka definicija osobnih podataka namjerna je i u biti se u Općoj uredbi o zaštiti podataka ne mijenja u usporedbi s prijašnjim zakonodavstvom[10]. Različitim aspektima definicije osobnih podataka, kao što su „svi podaci", „koji se odnose na", „utvrđen ili se može utvrditi", već se bavila Radna skupina iz članka 29.[11] u mišljenju 4/2007 od 20. lipnja 2007. o pojmu osobnih podataka, WP 136.

Pseudonimizacija osobnih podataka uobičajena je praksa u područjima kao što je istraživanje kako bi se prikrio identitet pojedinca. **Pseudonimizacija** je obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenoj osobi bez upotrebe dodatnih informacija. Te se dodatne informacije drže odvojeno i osigurane su organizacijskim ili tehničkim mjerama (npr. šifriranjem)[12,13]. Međutim, pseudonimizirani podaci i dalje se smatraju podacima o osobi koju se može identificirati ako se mogu pripisati toj osobi upotrebom dodatnih podataka[14]. Takvi se podaci **smatraju osobnim podacima** u skladu s Općom uredbom o zaštiti podataka.

Neosobni podaci

Ako podaci nisu „osobni podaci" kako su definirani u Općoj uredbi o zaštiti podataka, riječ je o **neosobnim podacima**. Neosobni podaci mogu se razvrstati prema podrijetlu na sljedeći način:

- Prvo, podaci koji izvorno nisu bili povezani s fizičkom osobom čiji je identitet utvrđen ili se može utvrditi, kao što su podaci o vremenskim uvjetima dobiveni senzorima ugrađenima na vjetroturbine ili podaci o potrebama za održavanjem industrijskih strojeva.

[10] Vidjeti članak 2. točku (a) Direktive 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (datum prestanka važenja: 24. svibnja 2018., stavljena izvan snage Općom uredbom o zaštiti podataka). Vidjeti i sudsku praksu Suda o definiciji osobnih podataka, kojom se prihvaća široko tumačenje tog pojma, primjerice presudu Suda od 29. siječnja 2009., *Productores de Música de España (Promusicae)*/*Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; presudu Suda od 24. studenoga 2011., C-70/10, *Scarlet Extended SA*/*Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; presudu Suda od 19. listopada 2016., *Patrick Breyer*/*Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

[11] Radna skupina iz članka 29. bila je Komisijino savjetodavno tijelo u području zaštite podataka te je sudjelovala u izradi usklađenih politika u području zaštite podataka u EU-u. Nakon što je Opća uredba o zaštiti podataka stupila na snagu 25. svibnja 2018., tu je radnu skupinu naslijedio Europski odbor za zaštitu podataka.

[12] Vidjeti članak 4. točku 5. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) u kojoj se definira „pseudonimizacija".

[13] Primjerice, u kontekstu istraživanja o učincima novog lijeka može se govoriti o pseudonimizaciji ako su osobni podaci sudionika u studiji u istraživačkoj dokumentaciji zamijenjeni jedinstvenim atributima (npr. brojem ili oznakom) i ako se drže odvojeno te su im dodijeljeni jedinstveni atributi u zaštićenom dokumentu (npr. u bazi podataka zaštićenoj lozinkom).

[14] Vidjeti uvodnu izjavu 26. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

- Drugo, podaci koji su prvotno bili osobni podaci, ali su kasnije **anonimizirani**[15]. „anonimizacija" osobnih podataka razlikuje se od pseudonimizacije (vidjeti prethodno navedeno) jer se pravilno anonimizirani podaci ne mogu pripisati određenoj osobi, čak ni upotrebom dodatnih podataka[16], te stoga nisu osobni podaci.

Procjena pravilnosti anonimizacije podataka ovisi o konkretnim i jedinstvenim okolnostima svakog pojedinačnog slučaja[17]. Iz primjera ponovne identifikacije navodno anonimiziranih skupova podataka vidljivo je da takva procjena može biti zahtjevna[18]. Kako bi se utvrdilo je li moguće utvrditi identitet pojedinca, potrebno je uzeti u obzir sva sredstva za koja se može razumno pretpostaviti da će ih voditelj obrade ili druga osoba izravno ili neizravno za tu svrhu upotrijebiti[19].

Primjeri neosobnih podataka:

- Podaci koji su u toj mjeri agregirani da se pojedinačni događaji više ne mogu utvrditi (npr. pojedinačna putovanja osoba u inozemstvo ili obrasci putovanja koji bi se mogli smatrati osobnim podacima) mogu se smatrati anonimnim podacima[20]. Anonimni podaci koriste se, na primjer, u statistikama ili u izvješćima o prodaji (npr. za procjenu popularnosti proizvoda i njegovih značajki).

---

[15] Vidjeti uvodnu izjavu 26. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) u kojoj se navodi da „Načela zaštite podataka stoga se ne bi trebala primjenjivati na anonimne informacije, odnosno informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi ili na osobne podatke koji su učinjeni anonimnima na način da se identitet ispitanika ne može ili više ne može utvrditi."

[16] Vidjeti presudu Suda od 19. listopada 2016., *Patrick Breyer/Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. Sud je zaključio da se adresa dinamičnog internetskog protokola (IP adresa) može smatrati osobnim podatkom čak i ako treća strana (npr. pružatelj internetskih usluga) posjeduje dodatne podatke, što bi omogućilo utvrđivanje identiteta pojedinca. Mogućnost utvrđivanja identiteta pojedinca mora biti sredstvo za koje se može razumno očekivati da će se izravno ili neizravno upotrijebiti za utvrđivanje identiteta pojedinca.

[17] Anonimizaciju podataka trebalo bi uvijek provoditi najsuvremenijim tehnikama anonimizacije.

[18] Za primjere ponovne identifikacije navodno anonimiziranih podataka vidjeti studiju o protoku podataka u budućnosti koju su za odbor ITRE Europskog parlamenta izradili Blackman, C., Forge, S.: *Data Flows – Future Scenarios: In-Depth Analysis for the ITRE Committee,* 2017., str. 22., okvir 2. (Protok podataka – izgledi za budućnost: Detaljna analiza za odbor ITRE). Dostupno na internetu na: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

[19] Vidjeti uvodnu izjavu 26. Uredbe (EU) 2016/679 (Opće uredbe o zaštiti podataka), u kojoj se navodi „Kako bi se utvrdilo je li po svemu sudeći izgledno da se upotrebljavaju sredstva za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir sve objektivne čimbenike, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir i tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj."

[20] Vidjeti dokument Radne skupine iz članka 29.: *Mišljenje 05/2014 o tehnikama anonimizacije*, doneseno 10. travnja 2014., WP216, str. 9.: „Samo ako voditelj obrade skupi podatke na razinu kada se pojedinačni slučajevi više ne mogu utvrditi, rezultirajući skup podataka može se kvalificirati kao anoniman. Na primjer: ako neka organizacija prikuplja podatke o pojedinačnim putovanjima, pojedinačni obrasci putovanja na razini slučaja i dalje bi se kvalificirali kao osobni podaci za bilo koju stranku, dok god voditelj obrade (ili bilo koja druga stranka) i dalje ima pristup originalnim podacima, čak i ako su iz skupa pruženog trećim strankama uklonjeni izravni identifikatori. Ali ako bi voditelj obrade obrisao neobrađene podatke i samo omogućio skupne statističke podatke trećim strankama na visokoj razini, poput ‚ponedjeljkom na ruti X ima 160 % više putnika nego utorkom', oni bi se kvalificirali kao anonimni podaci."

- Podaci o visokofrekventnom trgovanju u financijskom sektoru ili podaci o preciznoj poljoprivredi koji pomažu u praćenju i optimizaciji upotrebe pesticida, hranjivih tvari i vode.

Međutim, ako se neosobni podaci na bilo koji način mogu povezati s pojedincem, zbog čega se njegov identitet može izravno ili neizravno utvrditi, ti se podaci moraju smatrati osobnim podacima.

Na primjer, ako izvješće o kontroli kvalitete na proizvodnoj liniji omogućuje povezivanje podataka s određenim radnicima u tvornici (npr. onima koji određuju proizvodne parametre), ti se podaci smatraju osobnim podacima i primjenjuje se Opća uredba o zaštiti podataka. Ista se pravila primjenjuju ako zahvaljujući razvoju tehnologije i analitike podataka postane moguće pretvoriti anonimizirane podatke u osobne podatke. [21]

Budući da se definicija osobnih podataka odnosi na „fizičke osobe", skupovi podataka koji sadržavaju imena i podatke za kontakt pravnih osoba u načelu su neosobni podaci[22]. Međutim, u određenim situacijama oni mogu biti i osobni podaci[23]. Primjerice, ako je naziv pravne osobe jednak imenu fizičke osobe koja je njezin vlasnik ili ako se podaci odnose na fizičku osobu čiji je identitet utvrđen ili se može utvrditi[24].

2.2. Miješani skupovi podataka

Slobodnom kretanju podataka u EU-u različito se pristupa u Uredbi o slobodnom protoku neosobnih podataka i Općoj uredbi o zaštiti podataka.

Uredbom o slobodnom protoku neosobnih podataka utvrđuje se opća zabrana zahtjeva u pogledu lokalizacije podataka za neosobne podatke. Člankom 4. stavkom 1. te uredbe zabranjeni su zahtjevi u pogledu lokalizacije podataka osim ako su u skladu s načelom proporcionalnosti opravdani iz razloga javne sigurnosti.

Općom uredbom o zaštiti podataka osigurava se visoka razina zaštite osobnih podataka, ali i slobodno kretanje takvih podataka. U skladu s člankom 1. stavkom 3. te Uredbe slobodno

[21] Ako se osobni podaci nezakonito obrađuju ili ako se obradom na drugi način povređuju odredbe Opće uredba o zaštiti podataka, ispitanici (fizičke osobe) imaju pravo na temelju Opće uredbe o zaštiti podataka podnijeti pritužbu nacionalnom nadzornom tijelu (tijelu za zaštitu podataka) u EU-u ili zatražiti djelotvornu pravnu zaštitu pred nacionalnim sudom. Zadaće, nadležnosti i ovlasti nacionalnih nadzornih tijela utvrđene su u poglavlju VI. odjeljku 2. Opće uredbe o zaštiti podataka.

[22] U uvodnoj izjavi 14. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) navodi se „Ovom se Uredbom ne obuhvaća obrada osobnih podataka koji se tiču pravnih osoba, a osobito poduzetnika koji su ustanovljeni kao pravne osobe, uključujući ime i oblik pravne osobe i kontaktne podatke pravne osobe." Međutim, to treba tumačiti s obzirom na definiciju osobnih podataka iz članka 4. stavka 1. Opće uredbe o zaštiti podataka.

[23] Vidjeti presudu Suda Europske unije od 9. studenoga 2010. u spojenim predmetima *Volker und Markus Schecke GbR*, C-92/09 i *Hartmut Eifert*, C-93/09 / *Land Hessen*, ECLI:EU:C:2010:662, točku 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

kretanje osobnih podataka „ne ograničava se ni zabranjuje iz razloga povezanih sa zaštitom pojedinaca u pogledu obrade osobnih podataka.” Tim se dvjema uredbama zajedno omogućuje slobodno kretanje „svih” podataka u EU-u. Posebne odredbe detaljnije se razmatraju u odjeljcima 3.1. i 3.2.

Miješani skup podataka sastoji se od osobnih i neosobnih podataka. Miješani skupovi podataka čine većinu skupova podataka koji se upotrebljavaju u podatkovnom gospodarstvu i česti su zbog tehnološkog razvoja, među ostalim interneta stvari (tj. digitalnog povezivanja predmeta), umjetne inteligencije i tehnologija analitike velikih podataka.

Primjeri miješanih skupova podataka:

- porezna evidencija poduzeća, u kojoj se navodi ime i prezime te telefonski broj njegova glavnog direktora,
- skupovi podataka u bankama, posebno oni s podacima o klijentima i pojedinostima transakcija, kao što su usluge plaćanja (kreditne i debitne kartice), aplikacije za upravljanje odnosima s partnerima (PRM), ugovori o kreditiranju, dokumenti u kojima su podaci o fizičkim osobama pomiješani s podacima o pravnim osobama,
- anonimizirani statistički podaci istraživačkih institucija i neobrađeni podaci u obliku u kojem su izvorno prikupljeni, primjerice odgovori pojedinačnih ispitanika na pitanja iz statističkih istraživanja,
- baza znanja poduzeća o problemima u području IT-a i njihovim rješenjima na temelju pojedinačnih izvješća o informatičkim incidentima,
- podaci koji se odnose na internet stvari, pri čemu neki podaci omogućuju donošenje pretpostavki o osobama čiji je identitet moguće utvrditi (npr. prisutnost na određenoj adresi i obrasci upotrebe), i
- analiza operativnih podataka iz zapisnika proizvodne opreme u proizvodnoj industriji.

Primjer: usluge upravljanja odnosima s klijentima

Neke se banke za upravljanje odnosima s klijentima (CRM) koriste uslugama trećih strana, za čiju je provedbu nužno omogućiti pristup podacima klijenata u okruženju CRM-a. Podaci koji su dostupni u okruženju CRM-a obuhvaćaju sve podatke potrebne za učinkovito upravljanje interakcijom s klijentima, kao što su poštanska adresa i adresa elektroničke pošte, telefonski broj, proizvodi i usluge koje kupuju, izvješća o prodaji, uključujući agregirane podatke. Stoga ti podaci mogu uključivati i osobne i neosobne podatke klijenata.

Kad je riječ o miješanim skupovima podataka, Uredbom o slobodnom protoku neosobnih podataka[25] predviđeno je sljedeće:

„U slučaju skupova podataka koji se sastoje i od osobnih i od neosobnih podataka, Uredba se primjenjuje na neosobne podatke koji su dio skupa. Ako su osobni i neosobni podaci u skupu

[25] Članak 2. stavak 2. te uredbe

podataka neraskidivo povezani, ovom se Uredbom ne dovodi u pitanje primjena Uredbe (EU) 2016/679."

Drugim riječima, kad je riječ o skupu podataka koji se sastoji od osobnih i neosobnih podataka:

- Uredba o slobodnom protoku neosobnih podataka primjenjuje se na dio skupa podataka koji sadržava neosobne podatke,
- odredba o slobodnom protoku iz Opće uredbe o zaštiti podataka[26] primjenjuje se na dio skupa podataka koji sadržava osobne podatke, i
- ako su neosobni podaci i osobni podaci u skupu podataka „neraskidivo povezani", prava na zaštitu podataka i obveze koje proizlaze iz Opće uredbe o zaštiti podataka u potpunosti se primjenjuju na cijeli miješani skup podataka, što vrijedi i u slučaju da osobni podaci čine samo mali dio skupa podataka[27].

To je tumačenje u skladu s pravom na zaštitu osobnih podataka zajamčenim Poveljom Europske unije o temeljnim pravima[28] i uvodnom izjavom 8. Uredbe o slobodnom protoku neosobnih podataka[29]. U uvodnoj izjavi 8. te uredbe navodi se da „ova Uredba ne utječe na pravni okvir o zaštiti fizičkih osoba u pogledu obrade osobnih podataka .... te osobito na [Opću uredbu o zaštiti podataka] ... i direktive (EU) 2016/680 i 2002/58/EZ."

Praktičan primjer:

Poduzeće koje posluje unutar EU-a nudi svoje usluge putem internetske platforme. Poduzeća (klijenti) učitavaju svoje dokumente, koji sadržavaju miješane skupove podataka. Poduzeće koja učitava dokumente („voditelj obrade") mora se pobrinuti da se obrada provodi u skladu s Općom uredbom o zaštiti podataka. Poduzeće koje nudi usluge obrade skupa podataka u ime voditelja obrade („izvršitelj obrade") dužno je pohranjivati i obrađivati podatke u skladu s Općom uredbom o zaštiti podataka, na primjer kako bi se zajamčila odgovarajuća razina sigurnosti u vezi s podacima, uključujući i šifriranjem.

Pojam „neodvojivo povezan" nije definiran ni u jednoj od dviju uredbi[30]. U praksi to može značiti da određeni skup podataka sadržava osobne i neosobne podatke čije je razdvajanje nemoguće ili ga voditelj obrade smatra ekonomski neučinkovitim ili tehnički neizvedivim. Na primjer, poduzeće bi kupnjom sustava CRM i sustava za izvješćivanje o prodaji dupliciralo

[26] Članak 1. stavak 3. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka). Vidjeti i njezin odjeljak 3.2.

[27] Kao što se ističe u *Radnom dokumentu službi Komisije – Procjena učinka priložena dokumentu Prijedlog uredbe Europskog parlamenta i Vijeća o okviru za slobodan protok neosobnih podataka u Europskoj uniji* (SWD(2017) 304 final), dio 1/2, str. 3., „bez obzira na količinu osobnih podataka u miješanim skupovima podataka, potrebno je u potpunosti poštovati odredbe Opće uredbe o zaštiti podataka u odnosu na dio skupa podataka koji čine osobni podaci."

[28] Povelja Europske unije o temeljnim pravima, SL C 362, 26.10.2012., str. 391.

[29] Uvodna izjava 8. te uredbe.

[30] Uredba o slobodnom protoku neosobnih podataka i Opća uredba o zaštiti podataka.

svoje troškove za softver jer bi moralo kupiti zaseban softver za sustave CRM (osobni podaci) i sustave za izvješćivanje o prodaji (agregirani/neosobni podaci) na temelju podataka CRM-a.

Razdvajanjem skupa podataka vjerojatno bi se znatno smanjila i vrijednost tog skupa podataka. Osim toga, zbog promjenjive prirode podataka (vidjeti odjeljak 2.1.) teže je jasno razlikovati i stoga razdvojiti različite kategorije podataka.

Važno je napomenuti da se nijednom od dviju uredaba poduzeća ne obvezuju da razdvajaju skupove podataka koje nadziru ili obrađuju.

Stoga će se na miješani skup podataka općenito primjenjivati obveze voditelja obrade i izvršitelja obrade podataka i obveza poštovanja prava ispitanika u skladu s Općom uredbom o zaštiti podataka.

Obrada zdravstvenih podataka

Zdravstveni podaci mogu biti dio mješovitog skupa podataka. To su, primjerice, elektronička zdravstvena evidencija, podaci prikupljeni tijekom kliničkih ispitivanja ili skupovi podataka prikupljeni mobilnim aplikacijama za zdravlje i dobrobit (npr. aplikacijama kojima se mjeri naše zdravstveno stanje, podsjeća na uzimanje lijeka ili prati naša tjelesna kondicija)[31]. Zbog tehnološkog razvoja u tim je skupovima podataka sve teže točno razdijeliti osobne od neosobnih podataka. Zbog toga se takvi skupovi podataka moraju obrađivati u skladu s Općom uredbom o zaštiti podataka, a posebno u skladu s njezinim člankom 9., kojim se utvrđuje opća zabrana obrade posebnih kategorija podataka i iznimke od te zabrane (naime, u skladu s tom uredbom zdravstveni podaci smatraju se posebnom kategorijom podataka).

Podaci u miješanim skupovima podataka koji sadržavaju zdravstvene podatke mogu biti vrijedan izvor informacija, npr. za buduća medicinska istraživanja, za mjerenje nuspojava propisanih lijekova, u zdravstveno-statističke svrhe ili za razvoj novih zdravstvenih usluga ili liječenja. Međutim, pri provođenju početnih postupaka obrade i daljnjoj obradi podataka nužno je poštovati odredbe Opće uredbe o zaštiti podataka. Stoga svaka takva obrada zdravstvenih podataka mora biti pravno utemeljena[32], opravdana i sigurna te mora uključivati dostatne mjere zaštite.

Konačno, ključno je da postoji pravna sigurnost za pojedince i poduzeća te povjerenje u vezi s obradom podataka. To je iznimno važno i za podatkovno gospodarstvo. Ta se pravna sigurnost i povjerenje jamče spomenutim dvjema uredbama, kojima je cilj sačuvati slobodno kretanje podataka.

[31] Pri izradi i upotrebi mobilnih zdravstvenih aplikacija nužno je strogo poštovati odredbe Opće uredbe o zaštiti podataka. Odgovarajući zahtjevi detaljnije će se razraditi u Kodeksu ponašanja u pogledu privatnosti za mobilne zdravstvene aplikacije, koji je u izradi. Dodatne informacije na adresi: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

[32] Vidjeti članak 6. stavak 1. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

3. Slobodan protok podataka i uklanjanje zahtjeva u pogledu lokalizacije podataka

U ovom odjeljku detaljnije se govori o zahtjevima u pogledu lokalizacije podataka iz Uredbe o slobodnom protoku neosobnih podataka i načelu slobodnog kretanja podataka iz Opće uredbe o zaštiti podataka. Iako su te odredbe namijenjene državama članicama, poduzeća iz njih mogu saznati kako spomenute dvije uredbe utječu na slobodno kretanje svih podataka u EU-u.

3.1. Slobodan protok neosobnih podataka

Uredbom o slobodnom protoku neosobnih podataka[33] predviđeno je sljedeće: „Zahtjevi u pogledu lokalizacije podataka zabranjuju se, osim ako su u skladu s načelom proporcionalnosti opravdani iz razloga javne sigurnosti.”.

Zahtjevi u pogledu lokalizacije podataka definirani su[34] kao „bilo koja obveza, zabrana, uvjet, ograničenje ili drugi zahtjev koji je utvrđen zakonima ili drugim propisima država članica ili koji je rezultat općih i dosljednih administrativnih praksi u državi članici i u javnopravnim tijelima, među ostalim u području javne nabave, ne dovodeći u pitanje Direktivu 2014/24/EU kojom se propisuje obrada podataka na državnom području određene države članice ili sprečava obrada podataka u bilo kojoj drugoj državi članici[35]”.

Iz te je definicije vidljivo da mjere kojima se ograničava slobodno kretanje podataka u EU-u mogu biti raznovrsne. Ograničenja se mogu utvrditi zakonima, upravnim propisima i odredbama, ili pak rezultirati iz općih i dosljednih upravnih praksi. Nadalje, zabrana zahtjeva u pogledu lokalizacije podataka odnosi se i na izravne i na neizravne mjere koje bi mogle ograničiti slobodan protok neosobnih podataka.

Izravne mjere koje se odnose na zahtjeve u pogledu lokalizacije podataka mogu biti primjerice obveza pohranjivanja podataka na određenom zemljopisnom području (npr. poslužitelji se moraju nalaziti u određenoj državi članici) ili obveza pridržavanja jedinstvenih nacionalnih tehničkih zahtjeva (npr. podaci moraju biti u posebnom nacionalnom formatu).

Neizravne mjere koje se odnose na zahtjeve u pogledu lokalizacije podataka, usmjerene na ometanje obrade neosobnih podataka u drugim državama članicama, mogu biti raznovrsne. Primjerice, to može biti zahtjev obvezne upotrebe postrojenja koja su certificirana ili odobrena u određenoj državi članici ili drugi zahtjevi koji imaju za posljedicu otežavanje

[33] Članak 4. stavak 1. te uredbe.

[34] Članak 3. stavak 5. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

[35] Napominjemo da pravna nesigurnost o opsegu legitimnih i nelegitimnih zahtjeva u pogledu lokalizacije podataka dodatno ograničava mogućnosti koje su na raspolaganju gospodarskim subjektima i javnom sektoru u području lokalizacije obrade podataka (vidjeti uvodnu izjavu 4. Uredbe (EU) 2018/1807 Europskog parlamenta i vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji).

obrade podataka izvan određenog zemljopisnog područja ili državnog teritorija unutar Europske unije[36,37].

Pri procjenjivanju je li određena mjera neizravni zahtjev u pogledu lokalizacije podataka treba razmotriti konkretne okolnosti pojedinog slučaja.

U Uredbi o slobodnom protoku neosobnih podataka[38] spominje se pojam **javne sigurnosti** kako je naveden u sudskoj praksi Suda Europske unije. Pojmom „javne sigurnosti" „obuhvaćene su i unutarnja i vanjska sigurnost države članice[39], kao i pitanja javnog reda, posebno u svrhu olakšavanja istrage i otkrivanja kaznenih djela te kaznenog progona. Njime se podrazumijeva postojanje stvarne i dovoljno ozbiljne prijetnje koja utječe na jedan od temeljnih interesa društva[40], kao što su prijetnja funkcioniranju institucija i ključnih javnih službi i opstanku stanovništva te rizik od ozbiljnog narušavanja vanjskih odnosa ili mirnog suživota naroda, ili rizik po vojne interese.".

Nadalje, svaki zahtjev u pogledu lokalizacije podataka koji je opravdan razlozima javne sigurnosti mora biti proporcionalan. Prema sudskoj praksi Suda Europske unije načelo proporcionalnosti nalaže da donesene mjere budu prikladne za postizanje željenog cilja te da ne prelaze ono što je potrebno za tu svrhu[41].

Radi jasnoće, zabranom zahtjeva u pogledu lokalizacije ne dovode se u pitanje postojeća ograničenja iz zakonodavstva EU-a[42].

---

[36] Uvodna izjava 4. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

[37] Vidjeti dvije studije o zahtjevima u pogledu lokalizacije podataka provedene uoči donošenja Uredbe o slobodnom protoku neosobnih podataka: (1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market* (Omogućavanje prekograničnog protoka podataka na jedinstvenom digitalnom tržištu), SMART 2015/2016. Dostupno na internetu na: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 i (2) Time.lex, Spark Legal Network i Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions* (Prekogranični protok podataka na jedinstvenom digitalnom tržištu: studija o ograničenjima lokalizacije podataka), SMART 2015/0054. Dostupno na internetu na: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

[38] Uvodna izjava 19. te uredbe.

[39] Vidjeti primjerice presudu Suda od 23. studenoga 2010., *Land Baden-Württemberg*/*Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, točku 43. i presudu od 4. travnja 2017., *Sahar Fahimian*/*Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, točku 39.

[40] Vidjeti primjerice presudu Suda od 22. prosinca 2008., *Komisija Europskih zajednica*/*Republika Austrija*, C-161/07, ECLI:EU:C:2008:759, točku 35. i u njoj citiranu sudsku praksu te presudu od 26. ožujka 2009., *Komisija Europskih zajednica*/*Talijanska republika*, C-326/07, ECLI:EC:C:2009:193, točku 70. i u njoj citiranu sudsku praksu.

[41] Vidjeti primjerice presudu Suda od 8. srpnja 2010., *Afton Chemical Limited*/*Državni tajnik za promet,* C-343/09, ECLI:EU:C:2010:419, točku 45. i u njoj citiranu sudsku praksu.

[42] Vidjeti primjerice članak 245. stavak 2. Direktive 2006/112/EZ od 28. studenoga 2006. o zajedničkom sustavu poreza na dodanu vrijednost, kojim je predviđeno sljedeće „države članice mogu zahtijevati od poreznih obveznika koji imaju poslovni nastan na njihovom području da ih izvješćuju o mjestu pohrane ako se ono nalazi izvan njihovog područja". Taj se zahtjev međutim treba tumačiti u skladu s člankom 249. kojim je propisano sljedeće: „Kada porezni obveznik čuva račune koje izdaje ili prima elektroničkim putem, koji mu jamči izravan internetski pristup podacima, te kada je mjesto pohrane u državi članici koja nije država članica u kojoj on ima poslovni nastan, nadležna tijela države članice u kojoj on ima poslovni nastan imaju pravo, u smislu ove Direktive, pristupa tim računima elektroničkim putem, prijenosa i uporabe tih računa, unutar ograničenja

Štoviše, Uredbom o slobodnom protoku neosobnih podataka poduzećima se ne nameću nikakve obveze niti im se ograničava sloboda sklapanja ugovora i odlučivanje o lokaciji obrade podataka.

Od država članica zahtijeva se da pojedinosti o eventualnim zahtjevima u pogledu lokalizacije koji se primjenjuju na njihovu državnom teritoriju objavljuju na **jedinstvenoj nacionalnoj kontaktnoj točki na internetu** (nacionalne internetske stranice). Države članice te internetske stranice moraju ažurirati ili ažurirane podatke dostavljati središnjoj kontaktnoj točki osnovanoj u skladu sa zakonodavstvom EU-a[43]. Radi praktičnosti i kako bi se poduzećima omogućio brz pristup relevantnim informacijama u cijelom EU-u Komisija će poveznice na te kontaktne točke objaviti na portalu Vaša Europa[44].

3.2. Slobodan protok neosobnih podataka

Općom uredbom o zaštiti podataka[45] predviđeno je sljedeće: „Slobodno kretanje osobnih podataka unutar Unije ne ograničava se ni zabranjuje iz razloga povezanih sa zaštitom pojedinaca u pogledu obrade osobnih podataka.”.

Ako država članica propisuje zahtjeve u pogledu lokalizacije osobnih podataka zbog razloga koji nisu zaštita osobnih podataka, ti će se zahtjevi morati procijeniti s obzirom na odredbe o temeljnim slobodama i dopuštenim osnovama za odstupanje od tih sloboda prema Ugovoru o funkcioniranju Europske unije[46,47] i relevantnom zakonodavstvu EU-a, kao što su Direktiva o uslugama[48] i Direktiva o elektroničkoj trgovini[49].

Primjer:

Nacionalnim pravom propisano je da se računi za obračun plaća moraju nalaziti u određenoj državi članici zbog razloga povezanih s regulatornom kontrolom, koju provodi npr. nacionalno tijelo nadležno za oporezivanje. Takva bi nacionalna odredba bila izvan opsega članka 1. stavka 3. Opće uredbe o zaštiti podataka jer joj svrha nije zaštita osobnih podataka. Umjesto toga, trebala bi se procijeniti s obzirom na odredbe o temeljnim slobodama i

određenih propisima države članice u kojoj porezni obveznik ima poslovni nastan, te ukoliko to ta nadležna tijela zahtijevaju u svrhu kontrole.”

[43] Članak 4. stavak 4. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

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

[45] Članak 1. stavak 3. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

[46] Pročišćena verzija Ugovora o funkcioniranju Europske unije, SL C 326, 26.10.2012., str. 47.–390.

[47] Vidjeti i presudu Suda od 19. lipnja 2008., *Komisija Europskih zajednica/Veliko vojvodstvo Luksemburg*, C-319/06, ECLI:EU:C:2008:350, točke 90.–91.: Sud je zaključio da je obveza držanja na raspolaganju i zadržavanja određenih dokumenata u određenoj državi članici ograničenje slobode pružanja usluga; obrazloženje da je „tijelima općenito jednostavnije provoditi nadzorne zadaće” nije dovoljno.

[48] Direktiva 2006/123/EZ Europskog parlamenta i Vijeća od 12. prosinca 2006. o uslugama na unutarnjem tržištu, SL L 376, 27.12.2006., str. 36.–68.

[49] Direktiva 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine („Direktiva o elektroničkoj trgovini”), SL L 178, 17.7.2000., str. 1.–16.

dopuštenim osnovama za odstupanje od tih sloboda u skladu s Ugovorom o funkcioniranju Europske unije.

Općom uredbom o zaštiti podataka[50] utvrđeno je da države članice mogu odrediti uvjete, uključujući ograničenja, s obzirom na obradu genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje. Međutim, kako je navedeno u uvodnoj izjavi 53., takva nacionalna ograničenja ne bi smjela sprečavati slobodan protok osobnih podataka unutar EU-a ako se ti uvjeti primjenjuju na prekograničnu obradu takvih podataka. To je u skladu s člankom 16. Ugovora o funkcioniranju Europske unije, kojim je utvrđena pravna osnova za donošenje pravila povezanih s pravom na zaštitu osobnih podataka i sa slobodnim kretanjem tih podataka.

3.3. Područje primjene Uredbe o slobodnom protoku neosobnih podataka

Kako je već spomenuto, cilj je Uredbe o slobodnom protoku neosobnih podataka osiguravanje slobodnog protoka neosobnih podataka „u Uniji"[51]. Ta se uredba dakle ne primjenjuje na transakcije obrade podataka koje se obavljaju izvan EU-a i na zahtjeve u pogledu lokalizacije podataka koji se odnose na takvu obradu[52,53].

U skladu s njezinim člankom 2. stavkom 1. područje primjene te uredbe ograničeno je na obradu elektroničkih neosobnih podataka u EU-u:

(a) koja se pruža kao usluga korisnicima s boravištem ili poslovnim nastanom u EU-u, bez obzira na to ima li pružatelj usluga poslovni nastan u EU-u ili nema; ili
(b) koju provodi fizička ili pravna osoba s boravištem odnosno poslovnim nastanom u EU-u za vlastite potrebe.

Primjeri:

Članak 2. stavak 1. točka (a) Uredbe o slobodnom protoku neosobnih podataka:

- Pružatelj usluga u oblaku sa sjedištem u SAD-u pruža usluge obrade podataka klijentima s boravištem ili poslovnim nastanom u EU-u. Pružatelj usluga u oblaku svoju djelatnost obavlja s pomoću poslužitelja koji se nalaze na području EU-a, na kojima se pohranjuju i obrađuju podaci europskih klijenata. Pružatelj usluga u oblaku ne mora posjedovati infrastrukturu u EU-u, no može npr. unajmiti poslužiteljski kapacitet u EU-

[50] Članak 9. stavak 4. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

[51] Vidjeti članak 1. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

[52] Vidjeti uvodnu izjavu 15. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

[53] Pojam „obrada" široko je definiran (članak 3. stavak 2. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji) te bi se, kako je istaknuto u uvodnoj izjavi 17, ta uredba trebala primjenjivati na obradu u najširem smislu i obuhvaćati upotrebu svih vrsta sustava IT-a.

u. Na takvu obradu podataka primjenjuje se Uredba o slobodnom protoku neosobnih podataka.

- Pružatelj usluga u oblaku sa sjedištem u Japanu pruža svoje usluge europskim klijentima. Kapaciteti za obradu podataka kojima raspolaže pružatelj nalaze se u Japanu, gdje se odvijaju i sve aktivnosti obrade. U tom se slučaju ne primjenjuje Uredba o slobodnom protoku neosobnih podataka jer se sve aktivnosti obrade odvijaju izvan EU-a[54].

Članak 2. stavak 1. točka (b) Uredbe o slobodnom protoku neosobnih podataka:

- Malo novoosnovano europsko poduzeće iz države članice A odluči proširiti svoje poslovanje i otvori podružnicu u državi članici B. Kako bi smanjilo troškove, pohranu i obradu podataka centralizira na poslužitelju koji se nalazi u državi članici A. Država članica ne smije zabraniti takvu centralizaciju IT-a, osim ako je to opravdano javnom sigurnošću i u skladu je s načelom proporcionalnosti.

Iako se Uredba o slobodnom protoku neosobnih podataka ne primjenjuje ako se sve aktivnosti obrade neosobnih podataka odvijaju izvan EU-a, Opća uredba o zaštiti podataka mora se poštovati ako su u skup podataka uključeni osobni podaci. Pravila koja se primjenjuju na prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama na temelju Opće uredbe o zaštiti podataka moraju se poštovati u svakom slučaju[55].

3.4. Aktivnosti koje se odnose na unutarnju organizaciju država članica

Uredbom o slobodnom protoku neosobnih podataka države članice nisu obvezne eksternalizirati pružanje usluga povezanih s neosobnim podacima koje žele samostalno pružati ili organizirati na način koji ne uključuje ugovore o javnoj nabavi[56].

U članku 2. stavku 3. drugom podstavku Uredbe o slobodnom protoku neosobnih podataka navodi se:

---

[54] Napominjemo da se Uredba (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji ne odnosi na zahtjeve u pogledu lokalizacije podataka koje države članice propisuju za pohranu neosobnih podataka u trećim zemljama, koji mogu biti ugrađeni u nacionalni pravni poredak države članice. Da razjasnimo, Opća uredba o zaštiti podataka primjenjuje se na obradu osobnih podataka ispitanika u EU-u koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u EU-u ako su aktivnosti obrade povezane s: (a) nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje; (b) praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar Unije (vidjeti članak 3. stavak 2. Opće uredbe o zaštiti podataka).

[55] U odnosu na prijenos osobnih podataka trećim zemljama, upućujemo na stranice 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_hr i *Komunikacija Komisije Europskom parlamentu i Vijeću – Razmjena i zaštita osobnih podataka u globaliziranom svijetu*, COM/2017/07 final, dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017 %3A7 %3AFIN. Komisija je 23. siječnja 2019. donijela odluku o primjerenosti za Japan i time omogućila slobodan protok osobnih podataka između dvaju gospodarstava na osnovi snažnih jamstava zaštite.

[56] Uvodna izjava 14. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

„Ovom se Uredbom ne dovode u pitanje zakoni i drugi propisi koji se odnose na **unutarnju organizaciju** država članica i koji dodjeljuju ovlasti i odgovornosti **za obradu podataka**, i upravljanje provedbom tih ovlasti i odgovornosti, tijelima javne vlasti i javnopravnim tijelima, kako su definirana u članku 2. stavku 1. točki 4. Direktive 2014/24/EU[57], **bez ugovorne naknade privatnih stranaka**."[58]

Mogu postojati legitimni interesi kojima bi se moglo opravdati odabir te vrste „samostalnog pružanja" usluga obrade podataka, kao što je povjeravanje posla unutarnjim izvođačima ili uzajamni dogovori između javnih uprava. Kao tipičan primjer navest ćemo upotrebu „vladina oblaka" ili povjeravanje pružanja usluga obrade podataka za javne institucije i tijela centraliziranoj agenciji za IT.

Međutim, Uredbom o slobodnom protoku neosobnih podataka države članice se potiče da razmotre gospodarsku učinkovitost i druge dobrobiti korištenja vanjskih pružatelja usluga[59,60]. Čim nacionalna tijela počnu „eksternalizirati" obradu podataka uz ugovornu naknadu privatnim strankama i obrada se odvija u EU-u, takva obrada spada u područje primjene Uredbe o slobodnom protoku neosobnih podataka, što znači da se na opće i upravne prakse nacionalnih tijela primjenjuje načelo slobodnog protoka neosobnih podataka. Naime, nacionalna tijela moraju se suzdržati od uvođenja ograničenja u pogledu lokalizacije podataka, npr. u natječajima javne nabave[61].

4. Samoregulatorni pristupi kojima se podržava slobodan protok podataka

Samoregulacija pridonosi inovaciji i povjerenju među subjektima na tržištu i omogućuje bržu reakciju na tržišne promjene. U ovom odjeljku iznosi se pregled samoregulatornih inicijativa u području obrade osobnih i neosobnih podataka.

4.1. Prijenos podataka i promjena pružatelja usluga u oblaku

Jedan je od ciljeva Uredbe o slobodnom protoku neosobnih podataka izbjegavanje prakse ovisnosti o određenom pružatelju usluga. Do toga dolazi ako korisnici ne mogu promijeniti pružatelja usluga jer su njihovi podaci blokirani u sustavu određenog pružatelja usluga,

[57] Člankom 2. stavkom 1. podstavkom 4. Direktive 2014/24/EZ Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/EZ, SL L 94, 28.3.2014., str. 65.–242. utvrđeno je da „‚javnopravna tijela' znači tijela koja posjeduju sve od sljedećih značajki: (a) uspostavljena su posebno u svrhu zadovoljavanja potreba u općem interesu, a nisu industrijske ili trgovačke naravi; (b) imaju pravnu osobnost; i (c) većim dijelom financira ih država, regionalna ili lokalna tijela ili druga javnopravna tijela ili su podložna upravljačkom nadzoru od strane tih tijela ili imaju upravni, upraviteljski ili nadzorni odbor, a više od polovice članova tih odbora imenovala je država, regionalna ili lokalna tijela ili druga javnopravna tijela."

[58] U uvodnoj izjavi 13. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji navodi se da se tom uredbom ne dovodi u pitanje Direktivu 2014/24/EU.

[59] Uvodna izjava 14. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

[60] Vanjski pružatelj usluga bio bi svaki subjekt koji nije „javnopravno tijelo", kako je predviđeno člankom 2. stavkom 1. podstavkom 4. Direktive 2014/24/EZ Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/EZ, SL L 94, 28.3.2014., str. 65.–242.

[61] Uvodna izjava 13. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

primjerice zbog specifičnog formata podataka ili ugovornih odredaba, te se ne mogu prenijeti izvan sustava IT-a tog pružatelja usluga. Neometan prijenos podataka važan je kako bi korisnici mogli slobodno birati pružatelja usluga prijenosa podataka, čime se omogućuje učinkovito tržišno natjecanje.

Prenosivost podataka između poduzeća sve je važnija u raznim granama digitalne industrije, među ostalim u pružanju usluga u oblaku.

U skladu s člankom 6. Uredbe o slobodnom protoku neosobnih podataka Komisija potiče i olakšava izradu samoregulatornih kodeksa ponašanja na razini EU-a („kodeksi ponašanja”) kako bi se pridonijelo konkurentnom podatkovnom gospodarstvu. U skladu s tim člankom industrija može razviti samoregulatorne kodekse ponašanja koji se odnose na promjenu pružatelja usluga i prijenos podataka između različitih sustava IT-a.

Pri izradi takvih kodeksa ponašanja o prijenosu podataka treba uzeti u obzir više aspekata, naime:

- **najbolje prakse** za olakšavanje promjene pružatelja usluga i prijenosa podataka u strukturiranom, uobičajenom i strojno čitljivom formatu,
- **minimalne zahtjeve u pogledu informacija** kako bi se osiguralo da profesionalni korisnici prije sklapanja ugovora imaju na raspolaganju dovoljno detaljne i jasne informacije u vezi s postupcima, tehničkim zahtjevima, rokovima i naknadama koje se primjenjuju u slučaju kad profesionalni korisnik želi promijeniti pružatelja usluga ili prenijeti podatke natrag u vlastiti sustav IT-a,
- **pristupe programima certifikacije** radi bolje usporedivosti usluga u oblaku, i
- **planove komunikacije** namijenjene jačanju osviještenosti o kodeksima ponašanja.

Kad je riječ o tržištu usluga u oblaku, Komisija je potaknula osnivanje radnih skupina relevantnih dionika u okviru jedinstvenog digitalnog tržišta, unutar kojih se okupljaju stručnjaci za tehnologije u oblaku i profesionalni korisnici tih tehnologija, među ostalim mala i srednja poduzeća. Jedna od tih skupina (radna skupina SWIPO) trenutačno radi na samoregulatornim kodeksima ponašanja za prijenos podataka i promjenu pružatelja usluga u oblaku [62], a jedna druga skupina (radna skupina CSPCERT) bavi se sigurnosnom certifikacijom[63].

Radna skupina SWIPO izrađuje kodekse ponašanja koji obuhvaćaju sve vrste usluga u oblaku: infrastruktura kao usluga (IaaS), platforma kao usluga (PaaS) i softver kao usluga (SaaS).

Komisija očekuje da će se ti kodeksi ponašanja dopuniti **modelima ugovornih klauzula**[64]. Ti će modeli biti tehnički i pravno dovoljno specifični kako bi omogućili praktičnu provedbu i primjenu kodeksa ponašanja, što će biti iznimno važno za mala i srednja poduzeća. Planira se

[62] Radna skupina Cloud Switching and Porting Data Working Group.

[63] Radna skupina European Cloud Service Provider Certification Working Group. Vidjeti i odjeljak 4.3.

[64] Vidjeti uvodnu izjavu 30. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji.

da će se modeli ugovornih klauzula izraditi nakon kodeksa ponašanja (što bi se trebalo dovršiti do 29. studenoga 2019.).

U skladu s člankom 8. Uredbe o slobodnom protoku neosobnih podataka Komisija će ocijeniti provedbu te uredbe do 29. studenoga 2022. Ocijenit će se: i. učinak na slobodan protok podataka u Europi, ii. primjena uredbe, posebno na miješane skupove podataka, iii. proces ukidanja postojećih neopravdanih ograničenja u pogledu lokalizacije podataka u državama članicama te iv. tržišna učinkovitost kodeksa ponašanja u području prijenosa podataka i promjene pružatelja usluga u oblaku.

Pojam prenosivosti podataka i interakcija s Općom uredbom o zaštiti podataka

U objema uredbama[65] spominje se prenosivost podataka i cilj da se olakša prijenos podataka iz jednog informatičkog okruženja u drugo, bilo interno ili kod drugog pružatelja usluga. Prenosivošću podataka sprečava se ovisnost o određenom pružatelju usluga i potiče konkurentnost među pružateljima usluga. Međutim, te se uredbe razlikuju s obzirom na pristup pojmu prenosivosti kad je riječ o odnosu između ciljanih interesnih skupina i pravnoj naravi odredaba.

Pravo na prenosivost osobnih podataka u skladu s člankom 20. Opće uredbe o zaštiti podataka odnosi se na vezu između ispitanika i voditelja obrade. Riječ je o pravu ispitanika da zaprimi osobne podatke koje je pružio voditelju obrade, u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu, te o njegovu pravu da te podatke prenese drugom voditelju obrade ili na vlastite kapacitete za pohranu a da ga voditelj obrade kojem su osobni podaci bili pruženi u tome ne ometa[66]. Tipičan su primjer ispitanika korisnici raznih mrežnih usluga koji žele promijeniti svoje pružatelje usluga.

Člankom 6. Uredbe o slobodnom protoku neosobnih podataka nije predviđeno pravo profesionalnih korisnika na prijenos podataka, no predviđen je samoregulatorni pristup koji se temelji na dobrovoljnoj primjeni kodeksa ponašanja u tom sektoru. Istovremeno, pravo na prenosivost osobnih podataka odnosi se i na situaciju u kojoj je profesionalni korisnik eksternalizirao obradu svojih podataka trećoj strani koja pruža uslugu obrade podataka[67]. U skladu s člankom 3. stavkom 8. Uredbe o slobodnom protoku neosobnih podataka „profesionalni korisnik" može biti „fizička ili pravna osoba, uključujući tijelo javne vlasti ili javnopravno tijelo, koja koristi ili zatraži usluge obrade podataka za potrebe svoje trgovačke, poslovne, obrtničke ili profesionalne djelatnosti ili zadaće."

---

65 Članak 6. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018 o okviru za slobodan protok neosobnih podataka u Europskoj uniji i članak 20. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

66 Vidjeti dokument Radne skupine iz članka 29.: *Guidelines on the right to data portability* (Smjernice o pravu na prenosivost podataka). WP 242 rev.01, usvojen 13. prosinca 2016., kako je zadnje izmijenjen i usvojen 5. travnja 2017.

67 Uvodna izjava 29. Uredbe (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji. „Dok pojedinačni potrošači imaju koristi od postojećeg zakonodavstva Unije [tj. Opće uredbe o zaštiti podataka], promjena pružatelja usluga nije olakšana profesionalnim korisnicima koji to učine tijekom svoje poslovne ili profesionalne aktivnosti."

U praksi se prenosivost u skladu s člankom 6. Uredbe o slobodnom protoku neosobnih podataka odnosi na interakciju poduzeća, tj. profesionalnih korisnika (koji se u slučaju da obrađuju osobne podatke mogu smatrati „voditeljem obrade" u smislu Opće uredbe o zaštiti podataka) i pružatelja usluge (koji se u nekim slučajevima može smatrati „izvršiteljem obrade").

Unatoč razlikama, kad je riječ o miješanim skupovima podataka, može se dogoditi da se na prijenos podataka primjenjuju i Uredba o slobodnom protoku neosobnih podataka i Opća uredba o zaštiti podataka.

Primjer:

Poduzeće koje koristi usluge u oblaku odluči promijeniti pružatelja usluga u oblaku i prenijeti sve podatke novom pružatelju. Promjena pružatelja usluga i prijenos podataka obuhvaćeni su ugovorom između klijenta i pružatelja usluga u oblaku. Ako prijašnji pružatelj usluga u oblaku postupa u skladu s kodeksom ponašanja izrađenim na temelju Uredbe o slobodnom protoku neosobnih podataka, prijenos podataka mora se odviti u skladu s tamo navedenim zahtjevima.

Ako se u skupovima podataka nalaze i osobni podaci, taj prijenos mora biti u skladu s relevantnim odredbama Opće uredbe o zaštiti podataka, posebno u pogledu obveze da se novi pružatelj usluga u oblaku pridržava primjenjivih sigurnosnih i drugih zahtjeva[68].

Primjer:

Ako banka odluči promijeniti pružatelja usluge upravljanja odnosima s klijentima (CRM), neke (osobne i neosobne) podatke možda će trebati prenijeti s dotadašnjeg poslužitelja na novoga. Na te će se podatke primjenjivati različiti regulatorni zahtjevi, od kojih neki proizlaze iz Opće uredbe o zaštiti podataka, a neki iz Uredbe o slobodnom protoku neosobnih podataka.

4.2. Kodeksi ponašanja i programi certifikacije u području zaštite osobnih podataka

Kodeksi ponašanja i programi certifikacije mogu se upotrijebiti za dokazivanje usklađenosti s obvezama iz Opće uredbe o zaštiti podataka (vidjeti članak 24. stavak 3. i članak 28. stavak 5.).

U skladu s člankom 40. stavkom 1. i člankom 42. stavkom 1. Opće uredbe o zaštiti podataka države članice, nadzorna tijela, Europski odbor za zaštitu podataka i Komisija trebali bi poticati industriju da razvije kodekse ponašanja i uspostavi mehanizme certificiranja za zaštitu podataka.

[68] Vidjeti dokument Radne skupine iz članka 29.: *Mišljenje 05/2012 o računalstvu u oblaku* usvojeno 1. srpnja 2012., WP196, u kojem se dodatno pojašnjava položaj i dužnosti korisnika i pružatelja usluga u oblaku u vezi s obradom osobnih podataka.

Udruge i druga tijela koja čine zasebnu kategoriju voditelja ili izvršitelja obrade mogu pripremiti kodeks ponašanja za specifični sektor. Nacrt kodeksa mora se podnijeti na odobrenje nadležnom nadzornom tijelu[69]. Ako se nacrt kodeksa odnosi na aktivnosti obrade u više država članica, nadzorno tijelo ga prije odobrenja mora podnijeti Europskom odboru za zaštitu podataka. Odbor će tada dati svoje mišljenje o usklađenosti nacrta kodeksa s Općom uredbom o zaštiti podataka.

Europski odbor za zaštitu podataka objavio je Smjernice 1/2019 o kodeksima ponašanja i tijelima za praćenje u skladu s Općom uredbom o zaštiti podataka[70]. Te smjernice sadržavaju informacije o izradi kodeksa ponašanja, kriterijima za njihovo odobravanje i druge korisne informacije. Smjernice Europskog odbora za zaštitu podataka 1/2018 o certificiranju i utvrđivanju kriterija za certificiranje u skladu s člancima 42. i 43. Opće uredbe o zaštiti podataka sadržavaju informacije o certificiranju u skladu s tom uredbom te o izradi i odobravanju kriterija za certificiranje[71].

Primjeri kodeksa ponašanja koje je izradila industrija u oblaku:

EU-ov kodeks ponašanja za usluge u oblaku, čiju je izradu potaknula Komisija, izrađen je u suradnji sa skupinom Cloud Select Industry Group (C-SIG) na temelju Direktive o zaštiti podataka[72] i Opće uredbe o zaštiti podataka. Tim su kodeksom ponašanja obuhvaćene sve usluge u oblaku: softver kao usluga (SaaS), platforma kao usluga (PaaS) i infrastruktura kao usluga (IaaS)[73].

Kodeks ponašanja skupine CISPE[74] namijenjen je pružateljima infrastrukture kao usluge. Taj kodeks ponašanja sadržava zahtjeve koji se odnose na pružatelje infrastrukture kao usluge koji djeluju u svojstvu izvršitelja obrade podataka iz Opće uredbe o zaštiti podataka. Sadržava i odredbe o strukturi upravljanja za provedbu i primjenu kodeksa.

Kodeks ponašanja za usklađenost s Općom uredbom o zaštiti podataka koji je izradila skupina Cloud Security Alliance namijenjen je svim zainteresiranim dionicima iz područja računalstva u oblaku i europskog zakonodavstva u području zaštite osobnih podataka, kao što

[69] Članak 40. stavak 5. i članak 55. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

[70] Europski odbor za zaštitu podataka: Smjernice 1/2019 o kodeksima ponašanja i tijelima za praćenje u skladu s Uredbom 2016/679 (*Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*), usvojene 12. veljače 2019., verzija za javno savjetovanje, dostupne na sljedećoj adresi: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

[71] Europski odbor za zaštitu podataka: Smjernice 1/2018 o certificiranju i utvrđivanju kriterija za certificiranje u skladu s člancima 42. i 43. Uredbe 2016/679(*Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*, usvojene 23. siječnja 2019., dostupne na sljedećoj adresi: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

[72] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (datum prestanka važenja: 24. svibnja 2018.).

[73] Za više informacija o EU-ovu kodeksu ponašanja u oblaku vidjeti: https://eucoc.cloud/en/home.html

[74] Za više informacija o kodeksu ponašanja skupine CISPE vidjeti: https://cispe.cloud/code-of-conduct/

su pružatelji usluga u oblaku, klijenti i potencijalni klijenti u oblaku te nadzorna tijela i posrednici u tom sektoru. Kodeks ponašanja primjenjuje se na sve pružatelje usluga u oblaku[75].

4.3. Jačanje povjerenja u prekograničnu obradu podataka – certificiranje sigurnosti

Kako je navedeno u uvodnoj izjavi 33. Uredbe o slobodnom protoku neosobnih podataka, jačanjem povjerenja u sigurnost prekogranične obrade podataka trebala bi se smanjiti sklonost sudionika na tržištu i javnog sektora da pribjegavaju lokalizaciji podataka kao zamjeni za sigurnost podataka. Osim paketa o kibersigurnosti koji je Komisija predložila 2017.[76] radna skupina CSPCERT izrađuje smjernice za uspostavu Europskog programa za certificiranje usluga u oblaku, koje će zatim predstaviti Komisiji. Takav bi program mogao omogućiti slobodno kretanje podataka, bolju usporedivost i promicanje prihvaćenosti usluga u oblaku. Komisija može od ENISA-e (Agencije Europske unije za kibersigurnost) zatražiti da izradi pilot-program u skladu s odgovarajućim odredbama Akta o kibersigurnosti[77]. Tim bi se programom mogli obuhvatiti i osobni i neosobni podaci. Uz Akt o kibersigurnosti, kako je istaknuto u odjeljku 4.2., Opća uredba o zaštiti podataka može se upotrijebiti i kako bi se provjerilo postojanje odgovarajućih zaštitnih mjera u području sigurnosti podataka[78].

Završne napomene

Bez pravne sigurnosti i povjerenja u obradu podataka EU ne bi mogao iskoristiti puni potencijal podataka i razviti vrijednosne lance u svim sektorima i preko granica. Ta su pravna sigurnost i povjerenje zajamčeni spomenutim dvjema uredbama, koje imaju za cilj omogućavanje slobodnog kretanja podataka. Uredba o slobodnom protoku neosobnih podataka i Opća uredba o zaštiti podataka zajedno čine temelj za slobodan protok podataka u Europskoj uniji i vrlo konkurentno podatkovno gospodarstvo EU-a.

---

75 Za više informacija o kodeksu ponašanja skupine CSA vidjeti: https://gdpr.cloudsecurityalliance.org/

76 Više informacija potražiti na: https://ec.europa.eu/digital-single-market/en/cyber-security

77 Uredba Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agenciji Europske unije za kibersigurnost) i o sigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije te o stavljanju izvan snage Uredbe (EU) br. 526/2013 („Akt o kibersigurnosti")

78 Vidjeti uvodnu izjavu 74. Akta o kibersigurnosti.