

UREDBA (EU) 2018/1807 EUROPSKOG PARLAMENTA I VIJEĆA
od 14. studenoga 2018.
o okviru za slobodan protok neosobnih podataka u Europskoj uniji
(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacрта zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora ⁽¹⁾,

nakon savjetovanja s Odborom regija,

u skladu s redovnim zakonodavnim postupkom ⁽²⁾,

budući da:

- (1) Digitalizacija gospodarstva sve je brža. Informacijske i komunikacijske tehnologije više nisu poseban sektor, već temelj svih modernih inovativnih gospodarskih sustava. Elektronički podaci u središtu su tih sustava i njihovom analizom ili kombinacijom s uslugama i proizvodima može se generirati velika vrijednost. Istodobno brz razvoj podatkovnog gospodarstva i novih tehnologija kao što su umjetna inteligencija, proizvodi i usluge interneta stvari, autonomni sustavi i 5G otvaraju nova pravna pitanja u vezi s pristupom podacima i njihovoj ponovnoj upotrebi, odgovornosti, etici i solidarnosti. Trebalo bi predvidjeti poduzimanje koraka u području odgovornosti, posebno primjenom samoregulatornih kodeksa i drugih najboljih praksi, uzimajući u obzir preporuke, odluke i mjere poduzete bez ljudske interakcije duž cijelog vrijednosnog lanca obrade podataka. Takvi koraci mogli bi među ostalim uključivati odgovarajuće mehanizme za utvrđivanje odgovornosti, prenošenje odgovornosti među službama koje međusobno surađuju, osiguranje i reviziju.
- (2) Podatkovni vrijednosni lanci temelje se na različitim podatkovnim aktivnostima: stvaranju i prikupljanju podataka; objedinjavanju i organizaciji podataka; obradi podataka; analizi podataka te marketingu i distribuciji temeljenima na podacima; upotrebi i ponovnoj upotrebi podataka. Učinkovito i djelotvorno funkcioniranje obrade podataka ključna je sastavnica u svakom podatkovnom vrijednosnom lancu. Učinkovito i djelotvorno funkcioniranje obrade podataka i razvoj podatkovnog gospodarstva u Uniji priječe, međutim, dvije vrste prepreka mobilnosti podataka i jedinstvenom tržištu: zahtjevi u pogledu lokalizacije podataka koje primjenjuju nadležna tijela država članica i prakse ovisnosti o određenom pružatelju usluga u privatnom sektoru.
- (3) Sloboda poslovnog nastana i sloboda pružanja usluga iz Ugovora o funkcioniranju Europske unije (UFEU) vrijede i za usluge obrade podataka. Međutim određeni nacionalni, regionalni ili lokalni zahtjevi uvedeni u svrhu lokalizacije podataka na određenom području ometaju, a ponekad i sprečavaju pružanje tih usluga.
- (4) Takve prepreke za slobodno kretanje usluga obrade podataka te za pravo poslovnog nastana za pružatelje usluga proizlaze iz zahtjeva u pravima država članica da se za potrebe njihove obrade podaci lokaliziraju na određenom zemljopisnom ili državnom području. I neka druga pravila ili administrativne prakse imaju istovjetan učinak jer nameću posebne zahtjeve koji otežavaju obradu podataka izvan određenog zemljopisnog područja ili teritorija unutar Unije, kao što su zahtjevi da se upotrebljavaju tehnološka postrojenja certificirana ili odobrena u dotičnoj državi članici. Pravna nesigurnost u pogledu pitanja mjere legitimnih i nelegitimnih zahtjeva u pogledu lokalizacije podataka dodatno ograničava opcije dostupne sudionicima na tržištu i javnom sektoru u pogledu lokacije obrade podataka. Ovom se Uredbom ni na koji način ne ograničava sloboda poduzeća da sklapaju ugovore kojima se određuje gdje podaci trebaju biti locirani. Ovom se Uredbom samo nastoji očuvati tu slobodu tako što se osigurava da se dogovorena lokacija može nalaziti bilo gdje u Uniji.

⁽¹⁾ SL C 227, 28.6.2018., str. 78.

⁽²⁾ Stajalište Europskog parlamenta od 4. listopada 2018. (još nije objavljeno u Službenom listu) i Odluka Vijeća od 6. studenoga 2018.

- (5) Istodobno je mobilnost podataka u Uniji otežana i privatnim ograničenjima: problemima pravne, ugovorne i tehničke prirode koji ometaju ili sprečavaju korisnike usluga obrade podataka da svoje podatke prenesu od jednog pružatelja usluga drugome ili natrag u vlastite sustave informacijske tehnologije (IT), posebno po okončanju ugovora s pružateljem usluge.
- (6) Kombinacija tih prepreka dovela je do nedovoljnog tržišnog natjecanja između pružatelja usluga u oblaku u Uniji, do raznih problema povezanih s ovisnosti o određenom pružatelju usluga i do velikog nedostatka mobilnosti podataka. Isto tako, politikama lokalizacije podataka umanjuje se sposobnost poduzeća koja se bave istraživanjem i razvojem da potiču suradnju između poduzeća, sveučilišta i drugih istraživačkih organizacija s ciljem podupiranja inovacija.
- (7) Radi pravne sigurnosti i radi potrebe za jednakim uvjetima poslovanja na tržištu Unije, jedinstveni skup propisa za sve sudionike na tržištu ključan je čimbenik za funkcioniranje unutarnjeg tržišta. Kako bi se uklonile prepreke u trgovini i narušenost tržišnog natjecanja koji proizlaze iz razlika među nacionalnim pravima i spriječila pojava mogućih novih prepreka u trgovini i značajnog narušavanja tržišnog natjecanja, potrebno je donijeti jedinstvena pravila koja se primjenjuju u svim državama članicama.
- (8) Ova Uredba ne utječe na pravni okvir o zaštiti fizičkih osoba u pogledu obrade osobnih podataka i o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te osobito na Uredbu (EU) 2016/679 Europskog parlamenta i Vijeća ⁽¹⁾, direktive (EU) 2016/680 ⁽²⁾ i 2002/58/EZ ⁽³⁾ Europskog parlamenta i Vijeća.
- (9) Sve rasprostranjeniji internet stvari, umjetna inteligencija i strojno učenje predstavljaju glavne izvore neosobnih podataka, primjerice kada se koriste u automatiziranim procesima industrijske proizvodnje. Neki od konkretnih primjera neosobnih podataka jesu objedinjeni i anonimizirani skupovi podataka koji se koriste za analitiku velikih podataka, podaci o preciznoj poljoprivredi koji mogu pomoći pri praćenju i optimizaciji upotrebe pesticida i vode ili podaci o potrebama održavanja za industrijske strojeve. Bude li zahvaljujući tehnološkom razvoju anonimizirane podatke moguće pretvoriti u osobne podatke, s takvim se podacima treba postupati kao s osobnim podacima te se u skladu s time treba primjenjivati Uredba (EU) 2016/679.
- (10) U skladu s Uredbom (EU) 2016/679 države članice ne mogu ni ograničavati ni zabranjivati slobodan protok osobnih podataka unutar Unije iz razloga povezanih sa zaštitom pojedinca u vezi s obradom osobnih podataka. Ovom Uredbom utvrđuje se isto načelo slobodnog protoka unutar Unije za neosobne podatke, osim ako je ograničenje ili zabrana opravdana iz razloga javne sigurnosti. Uredbom (EU) br. 2016/679 i ovom Uredbom utvrđuje se koherentan skup pravila u vezi sa slobodnim protokom različitih vrsta podataka. Nadalje, ovom se Uredbom ne nameće obveza odvojenog pohranjivanja različitih vrsta podataka.
- (11) Kako bi se stvorio okvir za slobodan protok neosobnih podataka u Uniji i temelj za razvoj podatkovnog gospodarstva i jačanje konkurentnosti industrije Unije, neophodno je utvrditi jasan, sveobuhvatan i predvidiv pravni okvir za obradu podataka koji nisu osobni podaci na jedinstvenom tržištu. Pristup temeljen na načelima koji predviđa suradnju među državama članicama, kao i samoregulaciju, trebao bi osigurati dovoljnu fleksibilnost okvira za uzimanje u obzir novih potreba korisnika, pružatelja usluga i nacionalnih tijela u Uniji. Kako bi se izbjegao rizik preklapanja s postojećim mehanizmima, čime bi se izbjegla veća opterećenja i za države članice i za poduzeća, detaljna tehnička pravila ne bi trebalo uvoditi.
- (12) Ova Uredba ne bi smjela utjecati na obradu podataka ako se ona provodi kao dio aktivnosti koje su izvan područja primjene prava Unije. Osobito bi trebalo podsjetiti da je u skladu s člankom 4. Ugovora o Europskoj uniji (UEU) nacionalna sigurnost u isključivoj nadležnosti pojedine države članice.

⁽¹⁾ 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.).

⁽²⁾ Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. 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.).

⁽³⁾ 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.).

- (13) Slobodan protok podataka u Uniji imat će važnu ulogu u ostvarenju rasta i inovacija temeljenih na podacima. Tijela javne vlasti i javnopravna tijela država članica, jednako kao i poduzeća i potrošači, mogu imati koristi od veće slobode izbora u pogledu pružatelja podatkovnih usluga, od konkurentnijih cijena i veće učinkovitosti u pogledu pružanja usluga građanima. S obzirom na velike količine podataka koje tijela javne vlasti i javnopravna tijela obrađuju, od izuzetne je važnosti da ona služe kao primjer tako što će preuzeti usluge obrade podataka te da se suzdrže od ograničenja lokalizacije podataka kad se koriste uslugama obrade podataka. Stoga bi tijela javne vlasti i javnopravna tijela trebala biti obuhvaćena ovom Uredbom. U tom pogledu načelo slobodnog protoka neosobnih podataka koje predviđa ova Uredba trebalo bi se također primjenjivati na opće i dosljedne administrativne prakse i na druge zahtjeve u pogledu lokalizacije podataka u području javne nabave, ne dovodeći u pitanje Direktivu 2014/24/EU Europskog parlamenta i Vijeća ⁽¹⁾.
- (14) Kao u slučaju Direktive 2014/24/EU, ovom se Uredbom ne dovode u pitanje zakoni i drugi propisi koji se odnose na unutarnju organizaciju država članica, a kojima se dodjeljuju ovlasti i odgovornosti za obradu podataka i upravljanje provedbom tih ovlasti tijelima javne vlasti i javnopravnim tijelima bez ugovorne naknade privatnih stranaka. Premda se tijela javne vlasti i javnopravna tijela potiče na to da vode računa o financijskim i drugim koristima od eksternalizacije vanjskim pružateljima usluga, ona mogu imati opravdane razloge za odabir samostalnog pružanja usluga ili povjeravanja posla unutarnjim izvođačima. Posljedično tomu, nijednom se odredbom u ovoj Uredbi države članice ne obvezuje na podugovaranje ili eksternalizaciju pružanja usluga koje žele samostalno pružati ili organizirati na način koji ne uključuje ugovore o javnoj nabavi.
- (15) Ova bi se Uredba trebala primjenjivati na fizičke ili pravne osobe koje pružaju usluge obrade podataka korisnicima koji imaju boravište ili poslovni nastan u Uniji, uključujući pružatelje tih usluga koji pružaju usluge u Uniji ali nemaju poslovni nastan u njoj. Ova se Uredba stoga ne bi trebala primjenjivati na usluge obrade podataka koje se obavljaju izvan Unije i na zahtjeve u pogledu lokalizacije podataka koji se odnose na te podatke.
- (16) Ovom se Uredbom ne utvrđuju pravila u vezi s određivanjem mjerodavnog prava u trgovačkim stvarima te se stoga njome ne dovodi u pitanje Uredba (EZ) br. 593/2008 Europskog parlamenta i Vijeća ⁽²⁾. Konkretno, ako pravo koje je mjerodavno za ugovor nije odabrano u skladu s tom uredbom, ugovor o pružanju usluga u načelu je uređen pravom zemlje u kojoj pružatelj usluge ima uobičajeno boravište.
- (17) Ova bi se Uredba trebala primjenjivati na obradu podataka u najširem smislu, što obuhvaća upotrebu svih vrsta sustava IT-a, bez obzira na to jesu li oni locirani u prostorima korisnika ili eksternalizirani vanjskom pružatelju usluga. Ona bi trebala obuhvaćati obradu podataka različitih razina intenziteta, od pohrane podataka (engl. „Infrastructure-as-a-Service” (IaaS)) do obrade podataka putem platformi (engl. „Platform-as-a-Service” (PaaS)) ili u aplikacijama (engl. „Software-as-a-Service” (SaaS)).
- (18) Zahtjevi u pogledu lokalizacije podataka jasna su prepreka slobodnom pružanju usluga obrade podataka u cijeloj Uniji te funkcioniranju unutarnjeg tržišta. Kao takvi trebali bi biti zabranjeni, osim ako su opravdani iz razloga javne sigurnosti, kako je definirana pravom Unije, posebno u smislu članka 52. UFEU-a i ako zadovoljavaju načelo proporcionalnosti utvrđeno u članku 5. UEU-a. Kako bi se ostvarilo načelo slobodnog prekograničnog protoka neosobnih podataka, osiguralo brzo uklanjanje postojećih zahtjeva u pogledu lokalizacije podataka i iz operativnih razloga omogućila obrada podataka na više lokacija diljem Unije, te budući da se ovom Uredbom predviđaju mjere za osiguravanje dostupnosti podataka za potrebe regulatorne kontrole, države članice bi se trebale moći pozivati samo na javnu sigurnost kao opravdanje za zahtjeve u pogledu lokalizacije podataka.
- (19) Pojmom „javne sigurnosti” u smislu članka 52. UFEU-a i kako ga tumači Sud obuhvaćene su i unutarnja i vanjska sigurnost države članice, 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, 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. U skladu s načelom proporcionalnosti, zahtjevi u pogledu lokalizacije podataka koji su opravdani razlozima javne sigurnosti trebali bi biti primjereni postizanju željenog cilja te ne bi smjeli nadilaziti ono što je nužno za postizanje tog cilja.

⁽¹⁾ Direktiva 2014/24/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/18/EZ (SL L 94, 28.3.2014., str. 65.).

⁽²⁾ Uredba (EZ) br. 593/2008 Europskog parlamenta i Vijeća od 17. lipnja 2008. o pravu koje se primjenjuje na ugovorne obveze (Rim I), (SL L 177, 4.7.2008., str. 6.).

- (20) Kako bi se osigurala učinkovita primjena načela slobodnog prekograničnog protoka neosobnih podataka i spriječila pojava novih prepreka neometanom funkcioniranju unutarnjeg tržišta, države članice trebale bi Komisiji odmah dostaviti svaki nacrt zakona koji uvodi nove zahtjeve u pogledu lokalizacije podataka ili izmjene postojećeg zahtjeva u pogledu lokalizacije podataka. Ti nacrti zakona trebali bi se podnositi i ocjenjivati u skladu s Direktivom (EU) 2015/1535 Europskog parlamenta i Vijeća ⁽¹⁾.
- (21) Nadalje, kako bi se uklonile potencijalne postojeće prepreke, tijekom prijelaznog razdoblja od 24 mjeseca od datuma početka primjene ove Uredbe, države članice trebale bi provesti preispitivanje postojećih zakona i drugih propisa opće prirode kojima se utvrđuju zahtjevi u pogledu lokalizacije podataka i Komisiji dostaviti, uz obrazloženje opravdanosti, sve takve zahtjeve u pogledu lokalizacije podataka za koje smatraju da su u skladu s ovom Uredbom. To bi Komisiji trebalo omogućiti da ispita sukladnost svih preostalih zahtjeva u pogledu lokalizacije podataka. Komisija bi trebala moći, ako je to primjereno, davati primjedbe dotičnoj državi članici. Takve primjedbe bi mogle sadržavati preporuku o izmjeni ili ukidanju zahtjeva u pogledu lokalizacije podataka.
- (22) Obveza dostavljanja postojećih zahtjeva u pogledu lokalizacije podataka i nacrt zakona Komisiji, koja je uspostavljena ovom Uredbom, trebala bi se primjenjivati na regulatorne zahtjeve u pogledu lokalizacije podataka i nacrt akata opće prirode, ali ne na odluke upućene konkretnoj fizičkoj ili pravnoj osobi.
- (23) Kako bi se osigurala transparentnost zahtjeva u pogledu lokalizacije podataka u državama članicama utvrđenih u zakonima ili drugim propisima opće prirode za fizičke ili pravne osobe, kao što su pružatelji usluga i korisnici usluga obrade podataka, svaka država članica trebala bi putem jedinstvene nacionalne kontaktne točke na internetu objavljivati informacije o tim zahtjevima i redovito ažurirati te informacije. Alternativno bi države članice trebale ažurirane informacije o takvim zahtjevima dostavljati središnjoj kontaktnoj točki uspostavljenoj nekim drugim aktom Unije. Kako bi se na odgovarajući način informiralo fizičke i pravne osobe o zahtjevima u pogledu lokalizacije podataka u cijeloj Uniji, države članice trebale bi dostaviti Komisiji adrese tih jedinstvenih kontaktnih točaka. Komisija bi te informacije trebala objaviti na vlastitim internetskim stranicama, zajedno s redovito ažuriranim konsolidiranim popisom svih zahtjeva u pogledu lokalizacije podataka koji su na snazi u državama članicama, uključujući sažete informacije o tim zahtjevima.
- (24) Zahtjevi u pogledu lokalizacije podataka često proizlaze iz nepovjerenja u prekograničnu obradu podataka, a ono proizlazi iz pretpostavke da će u tom slučaju podaci biti nedostupni za nadležna tijela države članice za potrebe npr. inspekcije i revizije u svrhe regulatorne ili nadzorne kontrole. Takav problem nepovjerenja ne može se riješiti samo uz pomoć ništavnosti ugovornih uvjeta kojima se nadležnim tijelima zabranjuje zakonit pristup podacima u svrhu izvršavanja njihovih službenih dužnosti. Zato bi se ovom Uredbom trebalo jasno odrediti da ona ne utječe na ovlasti nadležnih tijela da zahtijevaju pristup podacima u skladu sa zakonodavstvom Unije ili nacionalnim zakonodavstvom, te da se nadležnim tijelima pristup podacima ne može odbiti uz obrazloženje da se podaci obrađuju u drugoj državi članici. Nadležna tijela mogla bi uvesti funkcionalne zahtjeve kako bi olakšala pristup podacima, primjerice zahtjev prema kojem opisi sustava trebaju biti u dotičnoj državi članici.
- (25) Fizičke ili pravne osobe koje podliježu obvezama dostave podataka nadležnim tijelima mogu takve obveze ispuniti omogućavanjem i jamstvom učinkovitog i brzog elektroničkog pristupa podacima za nadležna tijela, bez obzira na čijem državnom području se podaci obrađuju. Takav pristup podacima može se osigurati putem konkretnih uvjeta u ugovorima između fizičkih ili pravnih osoba koje podliježu obvezi davanja pristupa podacima i pružatelja usluga.
- (26) Ako fizička ili pravna osoba podliježe obvezi davanja pristupa podacima i ne ispunjava te obveze, nadležno tijelo bi trebalo moći zatražiti pomoć od nadležnih tijela u drugim državama članicama. U takvim slučajevima nadležna tijela bi trebala upotrebljavati posebne instrumente za suradnju utvrđene zakonodavstvom Unije ili međunarodnim sporazumima, ovisno o predmetu u dotičnom slučaju, kao što su, u području policijske suradnje, kaznenog ili građanskog pravosuđa odnosno u administrativnim stvarima, Okvirna odluka Vijeća

⁽¹⁾ Direktiva (EU) 2015/1535 Europskog parlamenta i Vijeća od 9. rujna 2015. o utvrđivanju postupka pružanja informacija u području tehničkih propisa i pravila o uslugama informacijskog društva (SL L 241, 17.9.2015., str. 1.).

2006/960/PUP⁽¹⁾, Direktiva 2014/41/EU Europskog parlamenta i Vijeća⁽²⁾, Konvencija o kibernetičkom kriminalu Vijeća Europe⁽³⁾, Uredba Vijeća (EZ) br. 1206/2001⁽⁴⁾, Direktiva Vijeća 2006/112/EZ⁽⁵⁾ i Uredba Vijeća (EU) br. 904/2010⁽⁶⁾. U nedostatku takvih posebnih mehanizama suradnje nadležna tijela trebala bi s ciljem osiguravanja pristupa traženim podacima međusobno surađivati putem uspostavljenih jedinstvenih kontaktnih točaka.

- (27) Ako zahtjev za pomoć sadržava zahtjev za pristup tijela primatelja zahtjeva svim prostorima fizičke ili pravne osobe, uključujući svu opremu i sredstva za obradu podataka, takav pristup mora biti u skladu s pravom Unije ili nacionalnim postupovnim pravom, uključujući i pravo zahtijevanja prethodnog sudskog odobrenja za pristup objektima.
- (28) Ovom se Uredbom korisnicima ne bi smjelo omogućiti da pokušaju izbjeći primjenu nacionalnog prava. Stoga bi njome trebalo predvidjeti da države članice mogu izricati učinkovite, proporcionalne i odvraćajuće sankcije korisnicima koji nadležnim tijelima onemogućuju pristup svojim podacima potrebnim za izvršavanje službenih dužnosti nadležnih tijela u skladu s pravom Unije i nacionalnim pravom. U hitnim slučajevima, kada korisnik zloupotrijebi svoje pravo, države članice trebale bi moći izricati strogo proporcionalne privremene mjere. Privremenim mjerama kojima se zahtijeva relokalizacija podataka na razdoblje dulje od 180 dana nakon relokalizacije odstupilo bi se od načela slobodnog kretanja podataka na dulje razdoblje te bi stoga o njima trebalo obavijestiti Komisiju radi ispitivanja njihove sukladnosti s pravom Unije.
- (29) Mogućnost prijenosa podataka bez prepreka ključni je čimbenik koji olakšava korisnikov odabir i učinkovito tržišno natjecanje na tržištima usluga obrade podataka. Stvarne ili prividne prepreke za prekogranični prijenos podataka također potkopavaju povjerenje profesionalnih korisnika u prekogranične ponude pa tako i povjerenje u unutarnje tržište. Dok pojedinačni potrošači imaju koristi od postojećeg zakonodavstva Unije, promjena pružatelja usluga nije olakšana profesionalnim korisnicima koji to učine tijekom svoje poslovne ili profesionalne aktivnosti. Usklađeni tehnički zahtjevi koji vrijede u cijeloj Uniji, neovisno o tome je li ta usklađenost postignuta tehničkim usklađivanjem, uzajamnim priznavanjem ili dobrovoljnim usklađivanjem, isto tako doprinose razvijanju konkurentnog unutarnjeg tržišta usluga obrade podataka.
- (30) Kako bi se u potpunosti iskoristile prednosti okruženja u kojem postoji slobodno tržišno natjecanje, profesionalni korisnici trebali bi moći donositi informirane odluke i lako uspoređivati pojedine komponente raznih ponuda usluga obrade podataka na tržištu, uključujući i u pogledu ugovornih uvjeta za prijenos podataka nakon prestanka ugovora. U cilju usklađivanja s potencijalom tržišta za inovacije te kako bi se u obzir uzelo iskustvo i stručno znanje pružatelja usluga i profesionalnih korisnika obrade podataka, detaljne informacije i operativne zahtjeve za prijenos podataka trebali bi definirati sudionici na tržištu samoregulacijom putem kodeksa ponašanja na razini Unije, koji bi mogli sadržavati modele ugovornih uvjeta, a Komisija bi to trebala poticati, olakšavati i nadzirati.
- (31) Kako bi promjene pružatelja usluga i prijenosi podataka zaživjeli i kako bi ih se olakšalo, takvi kodeksi ponašanja trebali bi biti sveobuhvatni i pokrivati barem ključne aspekte koji su važni tijekom postupka prijenosa podataka, i to postupke i lokaciju rezervnih kopija podataka, dostupne formate podataka te podršku, potrebnu konfiguraciju informacijske tehnologije i minimalnu širinu pojasa mreže, vrijeme potrebno prije pokretanja postupka prijenosa podataka i vrijeme tijekom kojeg će podaci ostati dostupni za prijenos te jamstva za pristup podacima u slučaju da pružatelj usluga proglasi stečaj. U kodeksima ponašanja trebalo bi također biti jasno utvrđeno da ovisnost o određenom pružatelju usluge ne predstavlja prihvatljivu poslovnu praksu, trebalo bi se omogućiti korištenje tehnologija za jačanje povjerenja te bi ih trebalo redovito ažurirati kako bi išli u korak s tehnološkim razvojem. Komisija bi se trebala pobrinuti za to da se u tom postupku provede savjetovanje sa svim relevantnim dionicima, uključujući udruženja malih i srednjih poduzeća (MSP-ovi) te novoosnovana poduzeća, korisnike i pružatelje usluga u oblaku. Komisija bi trebala ocijeniti izradu i učinkovitost provedbe takvih kodeksa ponašanja.

⁽¹⁾ Okvirna odluka Vijeća 2006/960/PUP od 18. prosinca 2006. o pojednostavljenju razmjene informacija i obavještajnih podataka između tijela zaduženih za izvršavanje zakona u državama članicama Europske unije (SL L 386, 29.12.2006., str. 89.).

⁽²⁾ Direktiva 2014/41/EU Europskog parlamenta i Vijeća od 3. travnja 2014. o Europskom istražnom nalogu u kaznenim stvarima (SL L 130, 1.5.2014., str. 1.).

⁽³⁾ Konvencija o kibernetičkom kriminalu Vijeća Europe, CETS br. 185.

⁽⁴⁾ Uredba Vijeća (EZ) br. 1206/2001 od 28. svibnja 2001. o suradnji između sudova država članica u izvođenju dokaza u građanskim ili trgovačkim stvarima (SL L 174, 27.6.2001., str. 1.).

⁽⁵⁾ Direktiva Vijeća 2006/112/EZ od 28. studenoga 2006. o zajedničkom sustavu poreza na dodanu vrijednost (SL L 347, 11.12.2006., str. 1.).

⁽⁶⁾ Uredba Vijeća (EU) br. 904/2010 od 7. listopada 2010. o administrativnoj suradnji i suzbijanju prijevare u području poreza na dodanu vrijednost (SL L 268, 12.10.2010., str. 1.).

- (32) Ako nadležno tijelo jedne države članice želi zatražiti pomoć druge države članice kako bi dobilo pristup podacima u skladu s ovom Uredbom trebalo bi putem uspostavljene jedinstvene kontaktne točke podnijeti obrazložen zahtjev jedinstvenoj kontaktnoj točki te države članice uključujući pismeno obrazloženje razloga i pravne osnove za traženje pristupa podacima. Jedinstvena kontaktna točka uspostavljena od strane države članice od koje je zatražena pomoć trebala bi olakšati prosljeđivanje zahtjeva relevantnom nadležnom tijelu države članice od koje je zatražena pomoć. Kako bi se osigurala učinkovita suradnja, tijelo kojem je zahtjev prosljeđen trebalo bi bez odlaganja pružiti pomoć kao odgovor na upućeni zahtjev ili dati informacije o poteškoćama s kojima se suoči prilikom udovoljavanja zahtjevu za pomoć ili o razlozima za njegovo odbijanje.
- (33) Jačanje povjerenja u sigurnost prekogranične obrade podataka trebalo bi smanjiti sklonost sudionika na tržištu i javnog sektora da pribjegavaju lokalizaciji podataka kao zamjeni za sigurnost podataka. Time bi se također trebala poboljšati pravna sigurnost za poduzeća u pogledu primjenjivih sigurnosnih zahtjeva ako aktivnosti obrade podataka eksternaliziraju pružateljima usluga, uključujući one u drugim državama članicama.
- (34) Sigurnosni zahtjevi u pogledu obrade podataka koji se primjenjuju na opravdan i proporcionalan način na temelju prava Unije ili nacionalnog prava u skladu s pravom Unije u državi članici boravišta ili poslovnog nastana fizičkih ili pravnih osoba čiji su podaci u pitanju trebali bi se primjenjivati i na pohranu i ostalu obradu tih podataka u drugoj državi članici. Te fizičke ili pravne osobe takve bi zahtjeve trebale moći ispuniti ili same ili putem klauzula u ugovorima s pružateljima usluga.
- (35) Sigurnosni zahtjevi uvedeni na nacionalnoj razini trebali bi biti neophodni i proporcionalni rizicima koji postoje za sigurnost obrade podataka u području primjene nacionalnog zakonodavstva u kojem su ti zahtjevi utvrđeni.
- (36) Direktivom (EU) 2016/1148 Europskog parlamenta i Vijeća ⁽¹⁾ utvrđene su mjere u cilju povećanja razine kibersigurnosti u Uniji. Usluge obrade podataka digitalne su usluge obuhvaćene tom direktivom. Prema toj direktivi države članice dužne su osigurati da pružatelji digitalnih usluga identificiraju rizike za sigurnost mrežnih i informacijskih sustava koje upotrebljavaju i poduzimaju odgovarajuće i proporcionalne tehničke i organizacijske mjere za upravljanje tim rizicima. Takvim mjerama trebalo bi osigurati razinu sigurnosti primjerenu postojećem riziku uzimajući u obzir sigurnost sustava i uređaja, nošenje s eventualnim incidentom, upravljanje kontinuitetom poslovanja, praćenje, reviziju i testiranje te sukladnost s međunarodnim standardima. Komisija te elemente treba detaljnije utvrditi provedbenim aktima u okviru te direktive.
- (37) Komisija bi trebala podnijeti izvješće o provedbi ove Uredbe, osobito u cilju određivanja potrebe za izmjenama s obzirom na tehnološki razvoj ili kretanja na tržištu. To bi izvješće naročito trebalo ocijeniti ovu Uredbu, prije svega njezinu primjenu na skupove podataka sastavljene od osobnih i neosobnih podataka, te provedbu izuzeća koje se odnosi na javnu sigurnost. Komisija bi prije početka primjene ove Uredbe trebala objaviti i informativne smjernice o postupanju sa skupovima podataka koji se sastoje od osobnih i neosobnih podataka kako bi poduzeća, uključujući MSP-ove, bolje razumjela interakciju između ove Uredbe i Uredbe (EU) 2016/670 i osigurala poštovanje obiju uredbi.
- (38) Ovom Uredbom poštuju se temeljna prava i postupaju se u skladu s načelima priznatima Poveljom Europske unije o temeljnim pravima te bi je trebalo tumačiti i primjenjivati u skladu s tim pravima i načelima, uključujući prava na zaštitu osobnih podataka, slobodu izražavanja i informiranja te slobodu poslovanja
- (39) S obzirom na to da cilj ove Uredbe, osiguravanje slobodnog protoka podataka koji nisu osobni podaci u Uniji, ne mogu dostatno ostvariti države članice, nego se, zbog njegova opsega i učinaka, on na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. UEU-a. U skladu s načelom proporcionalnosti utvrđenim u tom članku, ova Uredba ne prelazi ono što je potrebno za ostvarivanje tih ciljeva,

⁽¹⁾ Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

DONIJELI SU OVU UREDBU:

Članak 1.

Predmet

Cilj je ove Uredbe osigurati slobodan protok podataka koji nisu osobni podaci unutar Unije utvrđivanjem pravila koja se odnose na zahtjeve u pogledu lokalizacije podataka, dostupnost podataka za nadležna tijela i prijenos podataka za profesionalne korisnike.

Članak 2.

Područje primjene

1. Ova se Uredba primjenjuje na obradu elektroničkih podataka koji nisu osobni podaci u Uniji:
 - (a) koja se pruža kao usluga korisnicima s boravištem ili poslovnim nastanom u Uniji, bez obzira na to ima li pružatelj usluga poslovni nastan u Uniji ili izvan nje; ili
 - (b) koju provodi fizička ili pravna osoba s boravištem odnosno poslovnim nastanom u Uniji za vlastite potrebe.
2. 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 podataka neraskidivo povezani, ovom se Uredbom ne dovodi u pitanje primjena Uredbe (EU) 2016/679.
3. Ova se Uredba ne primjenjuje na aktivnost koja nije obuhvaćena područjem primjene prava Unije.

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, bez ugovorne naknade privatnih stranaka.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „podaci” znači podaci koji nisu osobni podaci kako su definirani u članku 4. točki 1. Uredbe (EU) 2016/679;
2. „obrada” znači svaki postupak ili skup postupaka koji se obavljaju na podacima ili skupovima podataka u elektroničkom formatu, bilo automatiziranim bilo neautomatiziranim sredstvima, kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, upotreba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;
3. „nacrt akta” znači tekst izrađen s ciljem donošenja u obliku općeg zakona ili drugog propisa, koji je još u fazi pripreme u kojoj i dalje postoji mogućnost unošenja suštinskih izmjena;
4. „pružatelj usluga” znači fizička ili pravna osoba koja pruža usluge obrade podataka;
5. „zahtjev u pogledu lokalizacije podataka” znači 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;
6. „nadležno tijelo” znači tijelo države članice, ili bilo koji drugi subjekt, koje je na temelju nacionalnog prava ovlašten obnašati javnu funkciju ili izvršavati službene ovlasti, ima ovlasti za pristup podacima koje obrađuju fizičke ili pravne osobe u svrhu obavljanja svojih službenih dužnosti, u skladu s pravom Unije ili nacionalnim pravom;
7. „korisnik” znači fizička ili pravna osoba, uključujući tijelo javne vlasti ili javnopravno tijelo, koja se koristi uslugama obrade podataka;
8. „profesionalni korisnik” znači 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.

Članak 4.

Slobodno kretanje podataka unutar Unije

1. Zahtjevi u pogledu lokalizacije podataka zabranjuju se, osim ako su u skladu s načelom proporcionalnosti opravdani iz razloga javne sigurnosti.

Prvim podstavkom ovog stavka ne dovodi se u pitanje stavak 3. ni zahtjevi u pogledu lokalizacije podataka utvrđeni na temelju postojećeg prava Unije.

2. Države članice u skladu s postupcima utvrđenima u člancima 5., 6. i 7. Direktive (EU) 2015/1535 Komisiji odmah dostavljaju svaki nacrt akta kojim se uvodi nov ili mijenja postojeći zahtjev u pogledu lokalizacije podataka.

3. Do 30 svibnja 2021. države članice dužne su osigurati stavljanje izvan snage svih postojećih zahtjeva u pogledu lokalizacije utvrđenih u zakonima ili drugim propisima koji nisu u skladu sa stavkom 1. ovog članka.

Do 30 svibnja 2021., ako država članica smatra da je postojeća mjera koja sadržava zahtjev u pogledu lokalizacije podataka u skladu sa stavkom 1. ovog članka i da stoga može ostati na snazi, o toj je mjeri dužna obavijestiti Komisiju uz obrazloženje opravdanosti zadržavanja tog zahtjeva na snazi. Ne dovodeći u pitanje članak 258. UFEU-a, Komisija u roku od šest mjeseci od dana primitka takve obavijesti ispituje usklađenost te mjere sa stavkom 1. ovog članka te, ako je to primjereno, daje komentare dotičnoj državi članici, uključujući prema potrebi davanje preporuke za izmjenu ili ukidanje mjere.

4. Svaka država članica putem jedinstvene nacionalne kontaktne točke na internetu ili, kada je to moguće, putem kontaktne točke na razini Unije utvrđene nekim drugim aktom Unije, objavljuje i redovito ažurira detalje o svim zahtjevima u pogledu lokalizacije podataka utvrđenim zakonima ili drugim propisima koji se primjenjuju na njezinu državnom području.

5. Svaka država članica obavješćuje Komisiju o adresi svoje jedinstvene kontaktne točke iz stavka 4. Poveznice na te jedinstvene kontaktne točke Komisija objavljuje na svojim internetskim stranicama, zajedno s redovito ažuriranim konsolidiranim popisom svih zahtjeva u pogledu lokalizacije podataka iz stavka 4., uključujući sažetak informacija o tim zahtjevima.

Članak 5.

Dostupnost podataka za nadležna tijela

1. Ova Uredba nema utjecaja na ovlasti nadležnih tijela da zatraže ili dobiju pristup podacima za potrebe obavljanja svojih službenih dužnosti u skladu s zakonodavstvom Unije i nacionalnim zakonodavstvom. Nadležnim tijelima ne može se odbiti pristup podacima uz obrazloženje da se obrađuju u nekoj drugoj državi članici.

2. Ako nadležno tijelo, nakon što je zatražilo pristup podacima korisnika, ne dobije taj pristup i ako u pravu Unije ili međunarodnim sporazumima ne postoji poseban mehanizam suradnje za razmjenu podataka među nadležnim tijelima različitih država članica, to nadležno tijelo može zatražiti pomoć od nadležnog tijela u drugoj državi članici u skladu s postupkom utvrđenim u članku 7.

3. Ako zahtjev za pomoć uključuje pristup nadležnog tijela kojem je zahtjev upućen svim prostorima fizičke ili pravne osobe, uključujući svu opremu i sredstva za obradu podataka, takav pristup mora biti u skladu s pravom Unije ili nacionalnim postupovnim pravom.

4. Države članice za nepoštovanje obveze davanja podataka mogu izreći učinkovite, proporcionalne i odvrćajuće sankcije, u skladu s pravom Unije i nacionalnim pravom.

U slučaju zloupotrebe prava koju je počinio korisnik, država članica tom korisniku može izreći strogo proporcionalne privremene mjere ako je to opravdano hitnošću pristupa podacima i uzimajući u obzir interese dotičnih stranaka. Ako se privremenom mjerom izrekne relokalizacija podataka na razdoblje dulje od 180 dana od relokalizacije, o njoj se Komisiju mora obavijestiti unutar tog roka od 180 dana. Komisija u najkraćem mogućem roku ispituje mjeru i njezinu usklađenost s pravom Unije te, ako je to primjereno, poduzima potrebne mjere. Komisija informacije o stečenom iskustvu razmjenjuje s jedinstvenim kontaktnim točkama država članica iz članka 7.

Članak 6.

Prijenos podataka

1. Komisija potiče i olakšava izradu samoregulatornih kodeksa ponašanja na razini Unije („kodeksi ponašanja”) kako bi se doprinijelo konkurentnom podatkovnom gospodarstvu utemeljenom na načelima transparentnosti i interoperabilnosti, u okviru kojeg se propisno uzimaju u obzir otvoreni standardi koji, među ostalim, obuhvaćaju sljedeće aspekte:
 - (a) najbolje prakse za olakšavanje promjene pružatelja usluga i prijenosa podataka u strukturiranom, uobičajenom i strojno čitljivom formatu, uključujući formate otvorenih standarda ako pružatelj usluga koji prima podatke to treba ili traži;
 - (b) minimalne zahtjeve u pogledu informacija kako bi se osiguralo da profesionalni korisnici imaju na raspolaganju dovoljno detaljne, jasne i transparentne informacije prije sklapanja ugovora o obradi podataka 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;
 - (c) pristupe programima certifikacije kojima se profesionalnim korisnicima olakšava uspoređivanje proizvoda za obradu podataka, uzimajući u obzir utvrđene nacionalne ili međunarodne norme kojima se olakšava usporedivost tih proizvoda i usluga. Ti pristupi mogu, među ostalim, obuhvaćati upravljanje kvalitetom, upravljanje informacijskom sigurnosti, upravljanje kontinuitetom poslovanja i upravljanje u području okoliša.
 - (d) planove komunikacijske u kojima se slijedi multidisciplinarni pristup kako bi se podigla osviještenost o kodeksima ponašanja među relevantnim dionicima.
2. Komisija osigurava da se kodeksi ponašanja izrađuju u uskoj suradnji sa svim relevantnim dionicima, uključujući udruženja MSP-ova i novoosnovanih poduzeća, korisnike i pružatelje usluga u oblaku.
3. Komisija potiče pružatelje usluga da dovrše izradu kodeksa ponašanja do 29. studenoga 2019. i da ih počnu učinkovito provoditi do 29. svibnja 2020.

Članak 7.

Postupak za suradnju među tijelima

1. Svaka država članica uspostavlja jedinstvenu kontaktnu točku koja se povezuje s jedinstvenim kontaktnim točkama ostalih država članica i Komisijom u pogledu primjene ove Uredbe. Države članice dužne su izvijestiti Komisiju o uspostavljenim jedinstvenim kontaktnim točkama i o svim daljnjim izmjenama u pogledu tih kontaktnih točaka.
2. Nadležno tijelo jedne države članice koje želi zatražiti pomoć druge države članice na temelju članka 5. stavka 2. kako bi dobilo pristup podacima podnosi obrazložen zahtjev jedinstvenoj kontaktnoj točki te države članice. Zahtjev mora sadržavati pismeno obrazloženje razloga i pravnu osnovu za traženje pristupa podacima.
3. Jedinstvena kontaktna točka identificira relevantno nadležno tijelo svoje države članice i tom nadležnom tijelu prosljeđuje zahtjev zaprimljen na temelju stavka 2.
4. Odgovarajuće nadležno tijelo koje je primilo zahtjev bez nepotrebnog odgađanja i u roku razmjernom hitnosti zahtjeva daje odgovor tako što dostavlja tražene podatke ili obavještuje nadležno tijelo koje zahtijeva podatke da ne smatra da su uvjeti za traženje pomoći iz ove Uredbe ispunjeni.
5. Sve informacije razmijenjene u kontekstu pomoći zatražene i pružene u skladu s člankom 5. stavkom 2. smiju se upotrebljavati samo u onu svrhu za koju su zatražene.
6. Jedinstvene kontaktne točke korisnicima pružaju opće informacije o ovoj Uredbi, uključujući o kodeksima ponašanja.

Članak 8.

Ocjena i smjernice

1. Komisija najkasnije 29. studenoga 2022. podnosi izvješće Europskom parlamentu, Vijeću i Europskom gospodarskom i socijalnom odboru s ocjenom provedbe ove Uredbe, a posebno u pogledu:
 - (a) primjene ove Uredbe, posebice na skupove podataka koji se sastoje od osobnih i neosobnih podataka s obzirom na tržišni i tehnološki razvoj koji bi mogao proširiti mogućnosti poništavanja anonimizacije podataka;

- (b) provedbe članka 4. stavka 1. u državama članicama, a posebno izuzeća koje se odnosi na javnu sigurnost; i
 - (c) izrade i djelotvorne provedbe kodeksa ponašanja te djelotvornog pružanja informacija od strane pružatelja usluga.
2. Države članice dostavljaju Komisiji podatke potrebne za pripremu izvješća iz stavka 1.
3. Komisija do 29. svibnja 2019. objavljuje informativne smjernice o interakciji između ove Uredbe i Uredbe (EU) 2016/679, posebice u pogledu skupova podataka koji se sastoje od osobnih i neosobnih podataka.

Članak 9.

Završne odredbe

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova se Uredba počinje primjenjivati šest mjeseci nakon objave.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Strasbourgu 14. studenoga 2018.

Za Europski parlament
Predsjednik
A. TAJANI

Za Vijeće
Predsjednica
K. EDTSTADLER