

Др Синиша ДОМАЗЕТ*

ПРАВНИ АСПЕКТИ ЧУВАЊА ПОДАТАКА У ВИРТУЕЛНОМ „ОБЛАКУ“ (КЛАУДУ) У СВЕТЛУ ОПШТЕ УРЕДБЕ 2016/679 ЕВРОПСКЕ УНИЈЕ О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ¹

Резиме

У Европској унији не постоји „кровни“ пропис којим се уређује чување података у клаудима, већ је то уређено већим бројем правних аката. Један од главних извора права у вези са чувањем података у клауду представља Уредба Европске уније о заштити појединца у вези са обрадом личних података и о слободном кретању таквих података, као и стављању ван снаге Директиве 95/46/ЕЗ. Уредба се примењује и на клауд провајдере са седиштем изван Уније. Истраживање је показало да ће клауд провајдери бити одговорни за своје поступке у вези са обрадом података о личности. За непоштовање одредаба Уредбе предвиђене су високе новчане казне до чак 20 милиона евра или 4% годишњег промета. Посебан проблем за клауд провајдере представљаће спровођење права на заборав, с обзиром да су локације података често непознате, као и велику покретљивост података у клауд окружењу. Клауд провајдери ће имати обавезу да процењују да ли је захтев за брисање података оправдан, што представља правно питање, и изискиваће значајне трошкове за клауд провајдере. Истраживањем је утврђено да је потребно детаљније уредити област преношења података између различитих клауд платформи, а показало се да ће мањи клауд провајдери имати тешкоће у вези са уговором са под-обрађивачима, с обзиром на строге захтеве Уредбе. Најзад, утврђено је да Уредбом нису детаљније уређена питања зашти-

* Универзитет Едуконс, Сремска Каменица, sdomazetns@gmail.com

1 Овај рад је део истраживачког пројекта под шифром 47009 (Европске интеграције и друштвено-економске промене привреде Србије на путу ка ЕУ), финансираног од стране Министарства просвете, науке и технолошког развоја Републике Србије.

те података псеудонимизацијом или шифровањем. У раду су коришћени нормативни метод и правно-логички методи индукције и дедуције.

Кључне речи: право, привреда, безбедност, лични подаци, Европска унија, клауд

І Увод

Све већи број предузећа користи данас виртуелни облак или клауд (енг. *cloudcomputing*) базирану инфраструктуру – виртуелне ресурсе који се - као сервис обезбеђују преко интернета². Постоје три основна типа клауд окружења: приватни, јавни и хибридни. Три основна модела сервиса у сваком од клауд окружења су: инфраструктура као сервис, платформа као сервис и софтвер као сервис. Сваки од ова три модела има различит утицај на примену безбедности у клауду и ниједна мера није универзално примењивана - сва три модела. Свака комбинација клауд сервиса носи посебан сет ризика и захтева посебне мере заштите. Безбедност као појам у својој основи подразумева расположивост (доступност овлашћеним лицима), интегритет (ненарушавање целовитости) и поузданост (поверљивост, обезбеђење од крађе). Безбедност у клауду такође мора да испуни ове основне захтеве, али и неке специфичне као што су: безбедност мреже од злонамерних активности споља, безбедност трансакција унутар датацентра и између корисника и датацентра, безбедност платформе односно софтверских апликација, заштиту чувања и складиштења података, сагласност са регулативом и прописима. Безбедност у клауду се може поделити у две базичне категорије: безбедност која се односи на клауд провајдере и безбедност која се тиче корисника. Провајдери морају обезбедити да њихова клауд архитектура буде безбедна, а подаци и апликације корисника заштићени. Корисници са своје стране морају бити сигурни да је клауд провајдер предузео све неопходне мере за заштиту њихових података³.

Ово посебно важи с обзиром на чињеницу да се правна заштита неретко разликује од државе до државе, а да хакери широм света могу на различите начине допрети до осетљивих личних или пословних података. Није редак случај ни да подаци похрањени у „облаку“ (клауду) буду компромитовани од стране професионалаца које су ангажовале конкурентске компаније или државе, чиме се прелази на тло индустријске

2 У раду ће бити коришћен термин клауд.

3 Ненад Вељковић, Безбедност у клауду, 2013, доступно на адреси: <https://pcpress.rs/bezbednost-u-cloud-u/>, 15.03.2019.

шпијунаже. За пословне кориснике клауд технологија предвиђа читав низ предности, укључујући обезбеђење флексибилности, приступ новим услугама, помоћ у дигиталној трансформацији, брзину развоја и трошковну ефикасност⁴.

Развој клаудинг-а је веома значајан и омогућио је бројне предности у складиштењу и чувању осетљивих личних и пословних података. Колико је значајна клауд инфраструктура, говори податак да ће удео клауда у рачунарским активностима предузећа порасти од садашњих 10% на 45% до 2026. године⁵.

Имајући у виду наведено, од великог значаја је да постоји *адекватна правна регулатива* која ће омогућити већу безбедност података, како физичких лица, тако и компанија. У тексту који следи, биће више речи о правној регулативи у вези са клауд технологијама.

II Преглед правне регулативе Европске уније у вези са чувањем података у клауду

Треба истаћи да на нивоу Европске уније не постоји један „кривни“ пропис којим се уређује области чувања података у клаудима (*cloud computing*), већ је ова материја уређена већим бројем аката секундарног законодавства ЕУ и одредбама националног законодавства. Један од главних извора права у вези са чувањем података у клауду представља *Уредба Европске уније о заштити појединца у вези са обрадом личних података и о слободном кретању таквих података, као и стављању ван снаге Директиве 95/46/ЕЗ* (Општа уредба о заштити података, у даљем тексту: Уредба)⁶.

Поред GDPR Уредбе, чување података у клауду уређено је, поред осталог, и у *Директиви 2016/1148 Европског парламента и Савета од 6. јула 2016. године о мерама за висок заједнички ниво безбедности мрежних и информационих система широм Уније*, потом у *Директиви 2002/58 Европског парламента и Савета од 12. јула 2002. године о обради личних података и заштити приватности у подручју електронских комуника-*

4 Richard Kemp, „Legal aspects of cloud security“, *Computer law & security review*, Vol. 34, Nr. 4/2018, 929.

5 David Floyer, „Cloud Vendor Revenue” Projections 2015-2026”, Wikibon, 2017, *доступно на адреси: <https://wikibon.com/cloud-vendor-revenue-projections-2015-2016/>*, 15.03.2019.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

ција (Директива о приватности и електронским комуникацијама), Директиви 2000/31/ЕЗ Европског парламента и Савета од 8. јуна 2000. године о одређеним правним аспектима услуга информационог друштва на унутрашњем тржишту, посебно електронске трговине (Директива о електронској трговини), Директиви 2009/22/ЕЗ Европског парламента и Савета од 29. априла 2009. године о судским налозима за заштиту интереса потрошача (кодификована верзија), Уредби (ЕУ) 2018/302 Европског парламента и Савета од 28. фебруара 2018. године о решавању питања неоправданог географског блокирања и других облика дискриминације на унутрашњем тржишту на основу држављанства, места боравишта или места пословног седишта клијената, те о измени Уредби (ЕЗ) бр. 2006/2004 и (ЕУ) 2017/2394 и Директиве 2009/22/ЕЗ, Директиве 2017/1564 Европског парламента и Савета од 13. септембра 2017. године о одређеним дозвољеним употребама одређених дела и других предмета заштите који су заштићени ауторским правом и сродним правима у корист лица која су слепи, која имају оштећење вида или имају других тешкоћа у коришћењу штампаних материјала и о измени Директиве 2001/29/ЕЗ о усклађивању одређених аспеката ауторског и сродних права у информационом друштву, Уредбе (ЕУ) 2017/1563 Европског парламента и Савета од 13. септембра 2017. године о прекограничној размени између Уније и трећих држава примерака у доступном формату одређених дела и других предмета заштите који су заштићени ауторским правом и сродним правима у корист лица која су слепи, која имају оштећење вида или имају других потешкоћа у коришћењу штампаних материјала, као и актима националних законодавстава држава чланица ЕУ. Поред наведених прописа, од значаја за *cloud-computing* је и *серија стандарда ISO 27000* (нарочито стандарди ISO 27001, 27108), ISO 38500 (*IT-управљање*), ISO/IEC 38505 (*управљање подацима*), и слично.

III Изазови у примени Опште Уредбе о заштити података на чување података у клауду

Област клаудинг-а је уређена са више одредаба Уредбе. Поменутом Уредбом се успостављају одређене обавезе за клауд провајдере. То подразумева да клауд провајдери имају уговорну одговорност. С тим у вези, треба нагласити да постоје два субјекта: клауд провајдер и клауд клијент. Клауд клијент би се могао сматрати лицем које (у складу са Уредбом) рукује подацима (руковалац података), док би се клауд провајдер требао сматрати обрађивачем података.

У пракси велики проблем представља чињеница да понекад није лако утврдити да ли је клауд провајдер руковалац или обрађивач података. У стварности, појединачни руковаоц података који користи услугу клауда обично не одређује сврху и средства на који начин ће лични подаци које он/она контролише бити обрађени. У клауд базама података, подаци се складиште међу серверима и другом опремом за складиштење података до којих корисници могу доћи уношењем одговарајућих креденцијала⁷. Информације и лични подаци се брзо преносе од једног центра за складиштење података ка другом и корисници немају контролу над средствима уз помоћ којих се подаци обрађују. Поред тога, постоје многе потрошачки усмерене клауд услуге, где су корисницима обезбеђене бесплатне услуге, док клауд провајдери користе сакупљене личне податке у циљу плаћања за услуге. У том контексту, провајдери клауд услуга би се (према слову Уредбе) могли означити као руковаоци података. Због тога се улога клауд провајдера мора истражити у сваком појединачном случају, у складу са природом клауд услуге⁸.

Према Уредби, провајдери клауд услуга морају да испуне читав низ обавеза, од којих се истичу обавеза вођења евиденције активности обраде за коју су одговорни⁹, обавеза примене одговарајућих техничких и организационих мера како би се постигао одговарајући ниво безбедности сходно ризику¹⁰, обавеза вршења процене утицаја предвиђених поступака обраде на заштиту података о личности¹¹, обавеза именовања овлашћеног лица за заштиту података о личности (*data protection officer*)¹², обавеза сарадње са надзорним органом на националном нивоу¹³.

Осим наведеног, у складу са чланом 5. поменуте Уредбе, лични подаци морају бити обрађивани на начин којим се обезбеђује одговарајућа безбедност личних података, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења

7 Christopher Milard, *Cloud computing Law*, 1st edition, Oxford, 2013, 3.

8 Peter Hustinx, European Data Protection Supervisor, Data protection and Cloud Computing under EU law, Third European Cyber Security Awareness Day, European Parliament, 13 April 2010, available at <http://www.edps.europa.eu>, in: Allesandro Mantelero, „Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution”, *European Journal of Law and Technology*, Nr.2/2012, 3.

9 Уредба, чл. 30.

10 Уредба, чл. 32.

11 Уредба, чл. 35.

12 Уредба, чл. 37.

13 Уредба, чл. 31.

применом одговарајућих техничких или организационих мера („целовитост и поверљивост“).

Даље, у делу Уредбе који се односи на обавезе руковооца обраде података, наводи се да, узимајући у обзир природу, опсег, контекст и сврхе обраде, као и ризике различитих нивоа вероватности и озбиљности за права и слободе појединаца, руковалац обраде ће спровести одговарајуће техничке и организационе мере како би обезбедио и могао доказати да се обрада спроводи у складу са овом Уредбом. Те се мере према потреби преиспитују и ажурирају¹⁴. У члану 25. Уредбе се наводи да, узимајући у најновија достигнућа, трошак спровођења као и природу, опсег, контекст и сврхе обраде, као и ризике различитих нивоа вероватности и озбиљности за права и слободе појединаца који произлазе из обраде података, руковалац обраде, и у време одређивања средстава обраде и у време саме обраде, спроводи одговарајуће техничке и организационе мере, попут псеудонимизације, за омогућавање ефикасне примене начела заштите података, као што је смањење количине података, као и укључење заштитних мера у обраду како би се испунили захтеви из ове Уредбе и заштитила права испитаника¹⁵.

Потом, област клаудинга је обухваћена и чланом 28(1) Уредбе, у коме се истиче даако се обрада спроводи у име руковооца, руковалацсе-користи једино обрађивачима који у довољној мери гарантују спровођење одговарајућих техничких и организационих мера на начин да је обрада у складу са захтевима из ове Уредбе и да се њом обезбеђује заштита права испитаника. Поменути члан је нарочито важан, јер се њиме уређује питање *уговорних обавеза између обрађивача и руковооца података*. С тим у вези, наводи се да се обрада од стране обрађивача уређује уговором или другим правним актом који је обавезујући за обрађивача у односу на руковооца. У поменутом уговору се дефинише предмет и трајање обраде, природа и сврха обраде, врста података о личности и категорије лица на која се подаци односе, као и обавезе и права руковооца. Уговором се дефинишу и *посебне уговорне обавезе за обрађивача*, као што су обавеза обезбеђења да се лица овлашћена за обраду података обавезу на поштовање поверљивости, обавеза предузимања адекватних мера за заштиту од губитка података, обавеза да се помаже руковооцу уз помоћ одговарајућих техничких и организационих мера у испуњавању обавезе руковооца да одговори на захтеве за остваривање права лица на која се подаци односе, обавеза да обрађивач по избору руковооца, брише или враћа руковоо-

14 Уредба, чл. 24(1).

15 Уредба, чл. 25(1).

цу све податке о личности након окончања пружања услуга у вези са обрадом и уништава постојеће копије, обавеза обрађивача да руковаоцу ставља на располагање све информације неопходне за доказивање поштовања обавеза и руковаоцу или другом ревизору којег овласти руковалац омогућава вршење ревизије, укључујући и инспекције, и помаже у њиховом вршењу, и слично¹⁶.

Посебно је важно решење Уредбе по којем је руковалац одговоран за радње обрађивача података. Тако, у складу са Уредбом, ако се обрада врши у име руковаоца, руковалац сарађује искључиво са обрађивачима који у довољној мери гарантују примену одговарајућих техничких и организационих мера, тако да обрада буде у складу са захтевима из Уредбе и да обезбеђује заштиту права лица на која се подаци односе¹⁷.

Уредбом је предвиђена и обавеза заједничких руковалаца података да међусобним договором одреде одговорности свакога од њих у циљу извршавања обавеза из уредбе, нарочито у вези са остваривањем права лица на која се подаци односе и дужности свакога од њих у погледу пружања информација. Лице на које се подаци односе може да остварујесвојаправа у односунасвакогруковаоца и противсвакогодњих¹⁸.

С обзиром да постоји тенденција да провајдери клауд услуга нуде услуге појединцима и крајњим корисницима, поставило се питање да ли ће провајдери клауд услуга бити обухваћени Уредбом. С тим у вези, у Уредби се наводи да се она не примењује на обраду података о личности коју врше физичка лица у току искључиво личне или кућне активности и због тога није повезана са професионалном или привредном делатношћу. Личне или кућне активности могу да обухватају кореспонденцију и поседовање адреса или друштвено умрежавање и активности на интернету које се врше у контексту таквих активности. Међутим, уредба се примењује на руковаоце или обрађиваче који пружају средства за обраду података о личности за такве личне или кућне активности¹⁹.

Посебан проблем за провајдере клауд услуга представља обавеза да се претходно да специјална или генерална писмена сагласност руковаоца другом под-обрађивачу података. Ово нарочито долази до изражаја када се клауд услуге обезбеђују преко већег броја под-обрађивача, чиме

16 Уредба, чл. 28.

17 Исто.

18 Уредба, чл. 26.

19 Уредба, тачка 18.

долази до повећаног ризика за обраду личних података у недозвољене сврхе. Разумљиво, под-обрађивач података мора, у складу са чланом 28. Уредбе, испуњавати исте обавезе у погледу заштите података о личности, као што би био случај у уговору између обрађивача и руковоаца података (посебно кад је реч о примени одговарајућих техничких и организационих мера), јер ће у случају неиспуњења обрађивач сносити одговорност за његове поступке и радње.

Директан утицај на клауд провајдере имају и два нова права која су загарантована Уредом: *право на брисање (право на заборав)* и *право на преносивост података*.

Кад је реч о *праву на брисање*, у члану 17. Уредбе се наводи да испитаник има право од руковоаца затражити брисање личних података који се на њега односе без непотребног одлагања, а руковалац има обавезу да обрише личне податке без непотребног одлагања, уколико је испуњен *макар један* од следећих услова: лични подаци више нису нужни у односу на сврхе за које су прикупљени или на други начин обрађени; испитаник повуче сагласност на којој се обрада заснива и ако не постоји друга правна основа за обраду; испитаник уложи приговор на обраду те не постоје јачи легитимни разлози за обраду, или испитаник уложи приговор на обраду у случају директног маркетинга; лични подаци су незаконито обрађени; лични подаци морају се брисати ради поштовања правне обавезе из права Уније или права државе чланице којем подлеже руковалац; лични подаци прикупљени су у вези с понудом услуга информационог друштва које се односе на децу²⁰.

С обзиром да су се појавили приговори да је овакво решење Уредбе у супротности са основним правима, као што је право на информисање или право говора, у Уредби је наведено да се право на брисање мора избалансирати са овим фундаменталним правима, уколико је то у сагласју са обавезама Уније или држава чланица, за потребе обављања задатака од значајног јавног интереса, из разлога јавног интереса у области јавног здравља, за потребе научног или историјског истраживања или статистичке потребе, и слично²¹.

За клауд провајдере је од посебног значаја део Уредбе (тачка 66), у којем се наводи да у циљу јачања „права на заборав“ у онлајн окружењу,

20 Синиша Домазет, Здравко Скакавац, „Право на заборав“ и Општа уредба Европске уније 2016/679 о заштити података о личности, *Европско законодавство*, бр. 66/2018, 79.

21 Уредба, чл. 23.

право на брисање треба да буде проширено тако да руковалац који је објавио податке о личности има обавезу да обавести руковоаоце података који такве податке обрађују да обришу све линкове за те податке о личности или копије или реконструкције тих података. Том приликом, руковалац мора да предузме одговарајуће мере, узимајући у обзир доступну технологију и средства доступна руковоаоцу података, укључујући и техничке мере, да обавести руковоаоце података који обрађују податке о личности о захтеву лица на које се подаци односе. Проблем представља чињеница да Уредба није прописала које су то „одговарајуће мере“, стога ће спровођење ове обавезе бити тежак задатак за клауд провајдере, посебно узимајући у обзир да подаци у отвореним мрежама, као што је интернет, могу бити копирани, постављени поново на различите локације, чињеницу да се често не може лако утврдити ко је руковалац или како да изворни руковалац открије друге руковоаоце. Ипак, постоје мишљења да је овакво решење Уредбе добро, јер ће руковоаоци морати добро да анализирају захтеве за брисање података о личности, с обзиром на високе санкције за кршење ове Уредбе²². Ипак, намеће се дилема да ли ће руковоаоци података (клауд провајдери) бити довољно стручни да решавају овако сложена питања.

Друго веома важно право предвиђено Уредбом односи се на *право на преносивост података*.

С тим у вези, лице на које се подаци односе има право да прими податке о личности који се односе на њега, а које је пружило руковоаоцу података у структурираном, уобичајеном и машински читљивом формату и има право да преноси те податке другом руковоаоцу података без ометања од стране руковоаоца којем су подаци о личности пружени уколико је обрада заснована на пристанку или уговору²³. Проблем представља чињеница да се клауд провајдери прилично разликују с обзиром на формате у којима чувају податке. Генерално, постоје бројни проблеми у вези са преносивошћу података, јер не постоји неки стандардни формат података који би био усвојен од стране свих клауд провајдера, нити интерфејси који омогућавају интероперабилност и преносивост података. Може се претпоставити да би велики клауд провајдери могли да издвоје финансијска средства за инвестирање у нове системе за трансфер података, али то би био

22 О овоме видети: Gilbert Francoise, "The Right of Erasure or Right to be Forgotten: What the Recent Laws, Cases, and Guidelines Mean for Global Companies", *Journal of Internet Law*, Nr. 8/2015, 1, 8; ML Rustad and S Kulevska, "Reconceptualising the Right to be Forgotten to Enable Transatlantic Data Flow", *Harvard Journal of Law & Technology*, Nr. 2/2015.

23 Уредба, чл. 20.

превелик терет за мале клауд провајдере. Постоје и мишљења да би „миграција“ података требала бити сматрана наплативом додатном услугом која би се нудила од стране клауд провајдера. То би могло створити ризик да велики клауд провајдери повећају трансакционе трошкове неопходне да се пређе од једне услуге на другу, и на тај начин би се њихови корисници „закључали“ у њиховим системима. Таква пракса би била сматрана злоупотребом доминантног положаја на тржишту²⁴.

Ипак, треба истаћи да је Уредбом забрањено да руковалац наплаћује било какву накнаду за достављање личних података, сем у случају да се ради о очигледно неоснованом или претераном захтеву или о захтеву који се пречесто подноси²⁵. Стога ће наплата таквих услуга бити везана само за појединачне случајеве (дефинисане Уредбом), али не и за сваки захтев који дође до клауд провајдера.

Посебан проблем у вези са услугама клауда јавља се у вези са *анонимизацијом* и *псеудонимизацијом података о личности*. У том смислу, наводи се да физичка лица могу да буду повезана са мрежним идентификаторима које пружају њихови уређаји, апликације, алати и протоколи, као што су адресе интернет протокола, идентификатори колачића или други идентификатори као што је ознака за радио-фреквенцијску идентификацију. То може да остави трагове који, посебно у комбинацији са јединственим идентификаторима и другим информацијама које примaju сервери, могу да се користе за профилисање физичких лица и њихову идентификацију²⁶. Дакле, што је дефиниција личних података шире постављена и уколико се они обрађују, утолико су веће шансе да се услуге клауд провајдера подведу под примену Уредбе. Треба узети у обзир и да корисници могу да шифрују њихове личне податке и да их затим поставе на клауд, тако да клауд провајдер нема никакав приступ кључу за дешифровање, па се не може ни поставити питање ризика по приватност²⁷. Дакле, намеће се дилема да ли ће обрађивач података моћи да се подведе под захтеве Уредбе, с обзиром да поседује личне податке, али без кључа за дешифровање? Другим речима, да ли ће се подаци који су учињени

24 Primavera De Filippi, Luca Belli, “Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation”, *European Journal for Law and Technology*, Nr. 2/2012, 6.

25 Уредба, чл. 12.

26 Уредба, тачка 30.

27 Kuan Hon, “Dark Clouds?”, *Intermedia Journal of the International Institute of Communications*, Nr. 4/2016, доступно на адреси: <http://www.iicom.org/intermedia/intermedia-past-issues/intermedia-january-2016/dark-clouds>, 20.03.2019.

анонимнима, псеудонимизовани или шифровани пре него што су постављени у кладу, бити сматрани личним подацима? Од одговора на ова питања зависи и правни положај клауд провајдера.

У Уредби се, поводом наведених питања, заузима став да начела заштите података не треба примењивати на анонимне информације, односно информације које се не односе на физичко лице чији је идентитет одређен или може да се одреди, или на податке о личности који су учињени анонимнима тако да идентитет лица на које се подаци односе не може да се одреди. Због тога се Уредба не односи на обраду таквих (анонимних) информација²⁸. Кад је реч о псеудонимизацији података, Уредба је дефинише као обраду података о личности на такав начин да подаци о личности више не могу да се повежу са конкретним лицем на које се подаци односе без коришћења додатних информација, под условом да се такве додатне информације чувају одвојено и да се на њих примењују техничке и организационе мере да би се обезбедило да подаци о личности не могу да се повежу са физичким лицем чији је идентитет одређен или се може одредити²⁹. Дакле, Уредба псеудонимизацију, као и шифровање, третира као меру заштите безбедности података. Такође, Уредба садржи својеврсне подстицаје за псеудонимизацију података о личности, наводећи да треба омогућити да исти руковалац може да спроводи мере псеудонимизације и општу анализу у случајевима када је тај руковалац предузео техничке и организационе мере потребне за обезбеђивање, у конкретној обради, ове уредбе, и одвојено чување додатних информација за приписивање података о личности одређеном лицу на које се подаци односе³⁰. На пример, уколико је дошло до компромитовања личних података одређеног лица, који су били заштићени, а да притом није дошло до компромитовања кључа за дешифровање, физичка лица не морају бити обавештена о томе.

Иако се у Уредби констатује да примена псеудонимизације на податке о личности може да смањи ризике за лица на која се подаци односе и да помогне руковооцима података и обрађивачима у испуњавању њихових обавеза у вези са заштитом података, то не искључује било које друге мере за заштиту података³¹.

28 Уредба, тачка 26.

29 Уредба, чл. 4.

30 Уредба, чл. 32. и тачка 29.

31 Уредба, тачка 28.

Дакле, анонимизацији, псеудонимизацији и шифровању података се у Уредби придаје велика пажња. Али, поставља се питање колики је стварни домашај ових одредби? Другим речима, да ли подаци који су учињени анонимним, псеудонимизовани или шифровани могу ипак бити идентификовани, с обзиром на све бржи развој информационо-комуникационих технологија и одговарајућих софтвера и алата који олакшавају процес идентификације? Одговор на ово питање је веома важан, јер ће од одговора зависити да ли ће обрада података потпасти под Уредбу или не. Иако Уредба захтева од руковоца података да примени одговарајуће организационе и техничке мере у циљу спречавања идентификације заштићених података о личности, треба узети у обзир да подаци који су учињени анонимним не потпадају под Уредбу, за разлику од анонимизованих података.

Како би се утврдило да ли идентитет физичког лица може да се одреди, треба узети у обзир сва средства, као што је издвајање, која ће руковалац или било које друго лице вероватно користити за непосредно или посредно одређивање идентитета физичког лица. Приликом процене која средства за одређивање идентитета физичког лица ће вероватно да буду употребљена, треба узети у обзир све објективне факторе, као што су трошкови и време потребно за утврђивање идентитета, узимајући у обзир технологију доступну приликом обраде и технолошки развој³².

У пракси се могу јавити одређене тешкоће приликом одговора на питање да ли је неко физичко лице могуће идентификовати, примера ради преко динамичке *IP*-адресе. Према схватању Суда правде у случају *Breyer*, динамичка *IP*-адреса ће се третирати као податак о личности уколико обрађивач података, у складу са националним правом, може тражити додатне информације од треће стране како би се физичко лице идентификовало. Стога се може закључити да је у Уредби прихваћен *објективни стандард* приликом процене могућности идентификације физичког лица на које се подаци односе.

Проблем представља и чињеница да развој модерних технологија све више отежава анонимизацију података о личности, то јест, идентификацију физичког лица чини лакшом. Самим тим, положај клауд провајдера на тржишту ће бити све комплекснији, јер ће то изискивати додатне трошкове за технологије које ће унапредити приватност корисника клауд услуга. Имајући у виду да клауд провајдери, махом, у својим

32 Уредба, тачка. 26.

условима коришћења услуге уопште не наводе одредбе о политици шифровања података, може се закључити да они неће хтети да обезбеде квалитетнију заштиту приватности корисника приликом обраде њихових личних података (посебно оних вредних), уколико не постоји одговарајућа правна регулатива која ће их обавезати на кораке у том правцу.

Још један велики проблем за клауд провајдере представља одредница да се Уредба може *примењивати и изван граница Уније*. О томе сведочи члан 3. Уредбе, у коме се наводи да се Уредба примењује на обраду података о личности у оквиру активности оснивања седишта руковооца или обрађивача у Унији, независно од тога да ли се обрада врши у Унији или не.

Овакав концепт није повољан за клауд провајдере. Разлог је у томе што клауд провајдери могу имати већи број центара за складиштење података, који су географски лоцирани у различитим државама чланицана Уније, а да се притом главно седиште клауд провајдера налази изван Уније. Због тога би у оваквом случају било јако тешко одредити који је центар за складиштење података представљао главно седиште. Ипак, уколико је руковалац (корисник клауд услуга) или обрађивач података (клауд провајдер) стационаран на територији Уније, тада ће се несумњиво применити решења Уредбе, чак и уколико се обрада врши ван граница Уније.

Такође, на клауд провајдере се може применити и одредба Уредбе којом се дефинише да се Уредба примењује на обраду података о личности лица на која се подаци односе у Унији коју врши руковалац или обрађивач који нема седиште у Унији, ако су активности обраде повезане са нуђењем робе или услуга таквим лицима на која се подаци односе у Унији, независно од тога да ли лице на које се подаци односе треба да изврши плаћање или праћењем њиховог понашања, под условом да се њихово понашање одвија унутар Уније³³. Ова одредба је нарочито важна, јер на тржишту постоје клауд сервиси који нуде робе или услуге корисницима, а притом прикупљају личне податке корисника ради лакшег плаћања њихових услуга³⁴.

Поставља се питање на који начин утврдити да ли руковалац података нуди робе или услуге корисницима у Унији. Према Уредби, треба утврдити да ли је очигледно да руковалац или обрађивач намерава да понуди услуге лицима на која се подаци односе и која се налазе у једној или више држава чланица Уније. Иако сама доступност интернет страна

33 Уредба, чл. 3.

34 На пример, један од таквих клауда се може пронаћи на следећем линку: <https://headspring.com/industries/consumer-goods-services/>

руковаоца, обрађивача или посредника у Унији или адресе електронске поште и других контакт података или коришћење језика који је уопштено у употреби у трећој земљи у којој руковалац има седиште нису довољни за утврђивање такве намере, фактори као што је коришћење језика или валуте који су уопштено у употреби у једној или више држава чланица уз могућност наручивања робе или услуга на том другом језику, или помињање купаца или корисника који се налазе у Унији, могу јасно да покажу такву намеру³⁵.

С друге стране, да би се одредило да ли активност обраде може да се сматра праћењем понашања лица на које се подаци односе, треба утврдити да ли се физичка лица прате на интернету, укључујући и могуће накнадно коришћење техника обраде података о личности које се састоје од профилисања физичког лица, посебно ради доношења одлука које се односе на њега или ради анализе или предвиђања његових личних склоности, понашања и ставова³⁶. Ова одредба је посебно значајна кад се говори о социјалним мрежама које прикупљају податке од корисника и продају их на тржишту, у циљу спровођења рекламних кампања.

Једно од најспорнијих питања у вези са применом Уредбе на клауд провајдере односи се на *прекогранични проток података о личности*, с обзиром да се подаци складиште на различитим локацијама, а обрада података складиштених у клауду се одвија у различитим јурисдикцијама широм света. Поред тога, клауд провајдери ретко обелодањују информације где складиште личне податке корисника, а национални прописи држава чланица у погледу заштите података о личности се могу разликовати. Проблем додатно компликује и чињеница да се највећи проценат клауд компанија налази у САД.

У складу са Уредбом, сваки пренос личних података који се обрађују или су намењени за обраду након преноса у трећу земљу или међународну организацију одвија се једино ако, у складу са другим одредбама ове Уредбе, руковалац и обрађивач делују у складу са условима који важе и за даље преносе личних података из треће земље или међународне организације у још једну трећу земљу или међународну организацију³⁷. Дакле, неовлашћени трансфер личних података (са клауда) је незаконит.

35 Уредба, тачка 23.

36 Уредба, тачка 24.

37 Уредба, чл. 44.

Уредба ограничава пренос личних података у трећу земљу или међународну организацију (дакле, ван ЕУ) уколико Комисија одлучи да трећа земља, територија, или један или више конкретних сектора унутар те треће земље или међународна организација не обезбеђује адекватан ниво заштите. Штавише, Уредбом се захтева да трећа земља треба да понуди гаранције којима се обезбеђује одговарајући ниво заштите који је суштински исти као ниво заштите обезбеђен у Унији, а посебно када се подаци о личности обрађују у једном или више конкретних сектора³⁸. Комисија је задржала право да периодично преиспитује раније донете одлуке о адекватности на сваке четири године, као и да спроводи мониторинг над развојем догађаја у трећим земљама или међународним организацијама. Уколико доступне информације указују да трећа земља, територија или један или више одређених сектора унутар треће земље или међународна организација више не обезбеђује адекватан ниво заштите, Комисија актима за спровођење ставља ван снаге, мења или суспендује одлуку³⁹.

У случају да одлука о адекватности није донета, руковацац или обрађивач може да пренесе податке о личности у трећу земљу или међународну организацију само ако су предвидели заштите мере, уколико то одобри Комисија или национално тело за заштиту података⁴⁰. Као одговарајуће заштите мере наводе се стандардне клаузуле о заштити података, као и обавезујућа корпоративна правила. Уколико су испуњени услови предвиђени Уредбом⁴¹, надлежно национално тело за заштиту података ће одобрити поменута правила. Ово је одредба која се свакако може применити у области услуга клауда. Када је реч о стандардним клаузулама за заштиту података, оне могу бити усвојене од стране Комисије, али се за њих не тражи сагласност националног тела за заштиту података. У погледу клауд провајдера, као добро решење би се могле навести модел клаузуле садржане у одлуци Комисије о стандардним клаузулама за пре-

38 Уредба, чл. 45; Уредба, т. 104.

39 Уредба, чл. 45(5). С тим у вези, јавио се велики проблем у односима између САД и ЕУ, јер је Унија сматрала да САД не обезбеђују адекватан ниво заштите личних података, услед великог „уплива“ америчких обавештајних служби у личне податке грађана (посебно услед случаја Едварда Сноудена). Слично је потврђено и у случају *Schrems*. Покушај да се пронађе излаз из ове ситуације је извршен склапањем такозваног „*EU-US Privacy Shield* споразума, али су сумње у адекватну заштиту остале и даље.

40 Уредба, чл. 46.

41 Уредба, чл. 47.

нос личних података обрађивачима у трећим земљама⁴², али треба нагласити да се ове клаузуле не могу применити на клауд провајдере који имају седиште изван ЕЗ, па је у том погледу неопходно извршити одговарајуће измене и допуне Уредбе.

Поред тога, Уредба наводи и одобрене кодексе понашања и одговарајуће механизме сертификације као облик заштитних мера⁴³, али треба нагласити да ове одредбе нису довољно прецизно регулисане, што такође представља својеврсни недостатак постојеће Уредбе и додатно усложњава положај клауд провајдера на тржишту.

Уколико не постоји одлука о адекватности, или одговарајуће заштите мере, пренос или скуп преноса података о личности у трећу земљу или међународну организацију врши се само под једним од услова одређених Уредбом. То подразумева да је лице на које се подаци односе изричито пристало на предложени пренос након што је упознато са могућим ризицима таквих преноса за лица на која се подаци односе због непостојња одлуке о адекватности и одговарајућих заштитних мера. Тај пристанак мора да се даје јасном потврдном радњом којом се изражава добровољан, конкретан, информисан и недвосмислен пристанак лица на које се подаци односе на обраду података о личности који се односе на њега, као што је писана изјава, укључујући и електронску изјаву, или усмена изјава⁴⁴. С друге стране, за осетљиве податке тражи се изричита сагласност⁴⁵. Ово ће бити јако тежак задатак за клауд провајдере, јер се услуге клаудинга врше на различитим локацијама, циљеви обраде података нису увек блиски клауд провајдерима, а истовремено се клауд провајдери сусрећу са великим бројем личних података корисника.

Још једна важна одредба Уредбе која се односи на клауд провајдере предвиђа да свака пресуда суда или трибунала и свака одлука органа управе треће земље којом се од руковоаца или обрађивача захтева пренос или откривање података о личности може бити призната или извршена на било који начин само ако се заснива на међународном споразуму, као што је уговор о узајамној правној помоћи, који је на снази између треће

42 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance), OJ L 39, 12.2.2010, p. 5–18.

43 Уредба, чл. 46.

44 Уредба, чл. 49; Уредба, тачка 32.

45 Уредба, чл. 9.

земље која је поднела захтев и Уније или државе чланице, не доводећи у питање друге разлоге за пренос⁴⁶. Дакле, уколико не постоји споразум о узајамној правној помоћи, откривање података о личности ће бити забрањено, осим уколико њихов пренос није у складу са условима постављених Уредбом.

Оно што ће свакако позитивно утицати на клауд провајдере, како са подручја Уније тако и ван ње, су *високе санкције за кршење Уредбе*. Тако, максимална казна која је предвиђена Уредбом износи 20 милиона евра или, у случају друштва, 4% укупног годишњег промета у свету за претходну финансијску годину, у зависности око тога који износ је већи⁴⁷. На овај начин, клауд провајдери (обрађивачи) ће бити директно одговорни према субјектима чије податке обрађују, док ће корисници података моћи да поднесу одговарајуће тужбе против клауд провајдера због неадекватне обраде њихових личних података, тражећи надокнаду штете. Та тужба би се могла поднети и против клауд провајдера који се налази ван Уније, с обзиром на поменута правила о екстериторијалности Уредбе. Клауд провајдери ће моћи да избегну одговорност једино уколико докажу да нису одговорни за штету која је наступила, што неће бити лак задатак.

IV Закључак

На основу реченог, може се закључити да су услуге чувања података у клауду у експанзији широм света. Имајући то у виду, Уредбом се настојало да се и ова област правно уреди и тако заштите интереси корисника података о личности. Она ће свакако значајно утицати на понашање клауд провајдера, који ће морати да предузму значајне кораке у заштити личних података, што до сада није био случај. Као значајан подстицај за промену понашања представља чињеница да ће клауд провајдери као обрађивачи података бити одговорни за своје понашање, уколико се неадекватном обрадом података о личности нанесе штета корисницима њихових услуга. То ће значити исплату значајних финансијских средстава на име одштете оштећеним субјектима, а ни казне за кршење Уредбе нису нимало занемарљиве (крећу се до чак 20 милиона евра, односно 4% годишњег промета ако је реч о друштвима).

Посебан проблем за клауд провајдере представљаће спровођење права на брисање (права на заборав), с обзиром да су локације података

46 Уредба, чл. 48.

47 Уредба, чл. 83.

често непознате, као и велику покретљивост података у клауд окружењу. Поред тога, клауд провајдери ће имати обавезу и да процењују да ли је захтев за брисање података оправдан, што представља правно питање, и изискиваће значајне трошкове за клауд провајдере. То је уједно и велика одговорност за клауд провајдере, посебно услед високих казни које им прете у случају доношења неодговарајуће одлуке. Не треба занемарити ни чињеницу да између различитих клауд платформи постоји инкомпатибилност, и да је преношење података у различитим форматима са једне клауд платформе на другу практично неизводљиво. Једини начин да се обезбеди међусобна интероперабилност јесте да се издвоје велика финансијска средства у нове технологије, што могу да обезбеде само велики клауд провајдери. Најзад, у погледу преноса података су могуће и одређене злоупотребе, јер се може очекивати да ће клауд провајдери намерно повећати висину накнаде за трошкове преноса података на другу платформу, како би „везали“ постојеће кориснике. Због тога, у решавање овог питања треба укључити и важеће одредбе из области права конкуренције ЕУ (нарочито у вези са злоупотребом доминантног положаја).

Додатну обавезу за клауд провајдере представља и подуговарање са обрађивачима, имајући у виду да Уредба прописује обавезујуће одредбе за овакве уговоре, а малим клауд провајдерима ће бити прилично тешко да испоштују наведене одредбе, чиме се примат даје већим играчима на тржишту клаудинг-а. На овај начин, доћи ће до повећања трошкова, што ће резултирати и повећањем цене услуга клаудинг-а и смањењем конкурентске снаге клауд провајдера из Уније.

Још једна тешкоћа за клауд провајдере односи се на питања псеудонимизације и анонимизације података. Уколико је обезбеђена одговарајућа заштита података (уз помоћ шифровања), тада неће бити одговорности клауд провајдера. Проблем је што у Уредби нису детаљније уређена ова питања, те се у будућности могу очекивати измене у том правцу.

На крају, екстериторијална примена Уредбе (и ван граница ЕУ) значиће да под Уредбу могу да потпадну и клауд провајдери ван Уније, што може изазвати бројне практичне проблеме. У сваком случају, високе казне које су предвиђене Уредбом несумњиво ће имати ефекат на понашање клауд провајдер и подићи ће стандарде у заштити података о личности.

Siniša DOMAZET

**LEGAL ASPECTS OF DATA STORAGE IN A VIRTUAL "CLOUD"
IN THE LIGHT OF GENERAL REGULATION 2016/679
OF THE EUROPEAN UNION FOR THE PROTECTION
OF PERSONAL DATA**

Resume

In the European Union there is no "roof" rule governing the storage of data in the cloud, but it is governed by a large number of legal acts. One of the main sources of law in connection with storing data in the cloud represents a Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. The Regulation also applies to cloud providers based outside the Union. Research has shown that cloud providers will be responsible for their actions in relation to the processing of personal data. For violating the provisions, the Regulation provides for high fines up to 20 million euro or 4% of annual turnover. A particular problem for cloud providers is implementation of the right to forgotten, considering that the location data is often unknown, and great mobility data in a cloud environment. Cloud providers will be required to assess whether the request for forgotten is justified, which is a legal issue, and will require significant costs for cloud providers. The research has found that it is necessary to further regulate transfer data between different cloud platforms, and that smaller cloud providers will have difficulties related to the contract with sub-processors, due to the strict requirements of the Regulation. Finally, it was found that the Regulation did not regulate data protection issues, such as pseudonymisation or encryption. The research used normative methods and legal and logical methods of induction and deduction.

Key words: law, economy, security, personal data, European Union, cloud.