

ZAŠTITA PODATAKA I NADLEŽNOSTI INSTITUCIJA EVROPSKE UNIJE

PRIRUČNIK

SADRŽAJ

PREDGOVOR.....	5
1. PRAVO NA ZAŠTITU PODATAKA O LIČNOSTI.....	9
Sudska praksa Evropskog suda za ljudska prava	14
1.1. Povelja EU o osnovnim pravima	18
Sadržaj.....	19
Oblast primene i tumačenje	20
Zaštita podataka o ličnosti.....	22
1.2. Direktiva 95/46/EZ.....	24
Sadržaj.....	24
1.3. Opšta uredba o zaštiti podataka	29
Sadržaj.....	30
Glavne promene.....	31
Diskusija i izazovi	38
2. ZAŠTITA PODATAKA I NADLEŽNOSTI INSTITUCIJA	
EVROPSKE UNIJE.....	41
2.1. Evropska komisija	43
Odgovornost	44
Službenik za zaštitu podataka	44
Schrems v Facebook.....	44
2.2. Radna grupa za zaštitu podataka Član 29.....	51
Pravni okvir.....	52
Mišljenja	53
Mišljenje 8/2014 o najnovijim kretanjima u oblasti interneta	
stvari	54
2.3. Evropski nadzornik za zaštitu podataka	68
Pravni okvir.....	69
Nadležnosti.....	69
Saradnja	70
Nadzor i sprovođenje	71
Prethodna procena rizika	72
Žalbe lica na koje se podaci odnose	73
Mišljenje 7/2015: Savladavanje izazova u vezi sa velikim	
podacima (<i>Big Data</i>).....	74

2.4. Agencija za osnovna prava Evropske unije.....	77
Nadležnosti.....	78
Delokrug rada	81
2.5. Evropski sud pravde	83
Sastav.....	84
Postupak	85
Presuda u spojenim predmetima C-293/12 i C-594/12 (<i>Digital Rights Ireland</i> i <i>Seitlinger</i> i ostali) od 8. aprila 2014.....	86
Presuda u predmetu C-131/12 (<i>Google Spain SL, Google Inc.</i> protiv <i>Agencia Española de Protección de Datos</i> , Mario Costeja González) od 13. maja 2014.....	90
Spojeni predmeti C-92/09 i C-93/09 <i>Volker und Markus</i> <i>Schecke GbR</i> i <i>Hartmut Eifert</i> protiv <i>Land Hessen</i> , presuda od 9. novembra 2010.....	95
2.6. Evropski Ombudsman	98
Predmeti	100
2.7. Evropol	103
Operativne aktivnosti.....	103
Upravljanje i kontrola	104
Zaštita podataka	104
Zajedničko nadzorno telo	106
Ciljevi	107
Centri	107
2.8. “Eurojust”	109
Nadležnosti.....	110
Globalni domet	113
Zajednički istražni timovi	114
Zajedničko nadzorno telo	114
Službenik za zaštitu podataka	116
Zaključak	117
3. BIBLIOGRAFIJA	119

PREDGOVOR



Zaštita podataka o ličnosti je izuzetno aktuelna tema koja utiče na svakodnevni život svakog od nas. Evropa ima jedan od sistema s najvišim stepenom zaštite u ovoj oblasti, zasnovan na Konvenciji 108 Saveta Evrope, instrumentima Evropske unije (EU) i sudskoj praksi Evropskog suda za ljudska prava (ESLJP) i Suda pravde Evropske unije (SPEU).

Namera ovog priručnika je da pruži jasan pregled institucija Evropske unije koje se bave zaštitom podataka. Institucije EU uređuju, vrše nadzor i donose sudske odluke u oblasti zaštite podataka i njihove nadležnosti su bliže opisane u nastavku teksta.

Cilj ovog priručnika je podizanje svesti i unapređenje znanja o pravilima zaštite podataka u državama članicama Evropske unije i Saveta Evrope. Stupanjem Lisabonskog ugovora na snagu u decembru 2009. godine, Povelja o osnovnim pravima EU postala je zakonski obavezujuća, a pravo na zaštitu podataka time je uzdignuto u status posebnog osnovnog prava. Bolje poznavanje Konvencije 108 Saveta Evrope i instrumenata EU, koji su utrli put zaštiti podataka u Evropi, kao i sudske prakse SPEU i ESLJP, od presudnog je značaja za zaštitu ovog osnovnog prava.

Nadamo se da će ovaj priručnik pomoći čitaocima da bolje razumeju ovo složeno ljudsko pravo i pružiti im pregled različitih institucija EU i njihovih nadležnosti u oblasti zaštite podataka o ličnosti.

Autori: dr Nataša Pirc Musar i Tina Kraigher Mišić

PRAVO

NA ZAŠTITU PODATAKA
O LIČNOSTI



Pravo na zaštitu podataka o ličnosti razvilo se iz prava na poštovanje privatnog života. Koncept privatnog života vezan je za ljudska bića. Shodno tome, fizička lica su primarni korisnici zaštite podataka. Dalje, prema mišljenju Radne grupe „Član 29“, zaštitu na osnovu evropskih propisa o zaštiti podataka uživaju samo živa bića.¹

Pravo na privatnost obuhvata takođe i podatke koji se odnose na lice. Ovakva prava razvila su se usled pojave i razvoja informacione tehnologije, koja je omogućila automatsku obradu podataka. Brz razvoj tehnologije i nekontrolisana obrada podataka ugrozili su pravo pojedinca na privatnost; štaviše, pravo na privatnost u vezi s podacima koji se isključivo odnose na pojedinca sve je ugroženije. Pravo na zaštitu podataka o ličnosti često se opisuje kao jedan od aspekata prava na privatnost – privatnost informacija pojedinca. Ono je takođe obuhvaćeno i Članom 8. Evropske konvencije o ljudskim pravima (EKLJP), koja predviđa pravo na poštovanje privatnog i porodičnog života kao deo prava na privatnost koje omogućava licu da uskrati pristup informacijama o sebi i zabranjuje drugim licima uvid u te informacije.

Zaštita podataka o ličnosti je garantovana fizičkom, ali ne i pravnom licu. Fizičko lice je zaštićeno od uplitanja države i drugih tela i organa iz javnog sektora, privrednih društava i drugih subjekata privatnog sektora; građani takođe uživaju zaštitu od uticaja drugih pojedinaca na osnovu privatnih ili javnih zbirki podataka o ličnosti. Naime, podacima o ličnosti smatraju se svi podaci koji se odnose na pojedinca, nezavisno od oblika u kojem su izraženi.

Stanovište EU o zaštiti podataka tesno je povezano s pitanjima privatnosti, što možda nije uvek najbolji pristup zaštiti podataka. Koncept privatnosti, kako je određen u Članu 8. EKLJP², odnosi se prvenstveno na pravo na privatni i porodični život, kao i poštovanje

¹ Radna grupa „Član 29“ (2007), Mišljenje 4/2007 o konceptu podataka o ličnosti, WP 136, 20. jun 2007, str. 22.

² Evropska konvencija o ljudskim pravima, ETS 5, Član 8.

stana i privatne korespondencije. Zaštita podataka može da obuhvata pitanja privatnosti, ali nije nužno ograničena samo na njih.³

Zaštita podataka podrazumeva pravo lica da bude upoznato sa tim koji se podaci o njemu prikupljaju, na koji način se podaci obrađuju, kako su zaštićeni i gde se prenose. Lice na koje se podaci odnose ima pravo uvida u te podatke i pravo da zahteva njihovu izmenu. Lice mora da dâ svoj pristanak da bi podatke moglo da koristi drugo lice, vlast ili subjekat. Vrednosti zaštite podataka nisu suštinski vezane za privatnost. Tim vrednostima se ne može pristupiti isključivo sa stanovišta privatnosti. U pitanju su samostalne vrednosti koje pružaju osnovna prava: pravo na zaštitu podataka, koje je priznato u Članu 8. Povelje o osnovnim pravima Evropske unije⁴:

Svako ima pravo na zaštitu podataka o svojoj ličnosti. Takvi podaci moraju biti obrađeni pošteno za tačno određenu svrhu, na osnovu pristanka lica na koje se podaci odnose ili po nekom drugom osnovu utvrđenom zakonom. Svako ima pravo da pristupi prikupljenim podacima o svojoj ličnosti i pravo da zatraži njihovu ispravku.

Prepoznavanje zaštite podataka u zakonskom okviru EU predstavlja važan korak ka priznavanju Direktive o zaštiti podataka⁵, za koju se godinama smatra da ima dva glavna atributa: omogućavanje i zaštitu slobodnog kretanja podataka o ličnosti i zaštitu osnovnih prava i sloboda pojedinca (sa stanovišta privatnosti).

Može se smatrati da, priznavanjem prava na zaštitu podataka u skladu s Poveljom⁶, dimenzija Direktive⁷ koja se odnosi na osnovna

³ D. Manolescu, Data protection as a fundamental right, dostupno na adresi: http://effectus.com/yahoo_site_admin/assets/docs/Data_protection_as_a_fundamental_right_Dan_Manolescu_Issue5.16761659.pdf (pristupljeno 14. 3. 2017).

⁴ Povelja o osnovnim pravima Evropske unije, 7. decembar 2000, Službeni list Evropskih zajednica, 18. decembar 2000 (2000/C 364/01), Poglavlje II, Član 8.

⁵ Direktiva 95/46/EZ Evropskog parlamenta i Saveta, od 24. oktobra 1995, o zaštiti pojedinca prilikom obrade podataka o ličnosti i o slobodnom kretanju tih podataka, SL list L281, 23. novembar 1995, str. 31 (Direktiva 95/46/EZ).

⁶ Povelja o osnovnim pravima Evropske unije, Poglavlje II, Član 8.

⁷ Direktiva 95/46/EZ.

prava dobija na težini. Neke zemlje u EU, poput Francuske i Nemačke, ne smatraju da je privatnost vezana za zaštitu podataka. Nasuprot tome, neke druge zemlje, kao što su Belgija i Holandija, tesno povezuju zaštitu podataka s privatnošću. Iz tog razloga bi priznavanje zaštite podataka kao pojedinačne slobode moglo da doprinese smanjenju razlika u tumačenju koje u ovoj oblasti postoje među državama članicama EU.⁸

Nažalost, zakonski okvir EU koji se odnosi na zaštitu podataka je prilično fragmentiran. Direktive koje uređuju oblast zaštite podataka (Direktiva 95/46/EZ⁹, Direktiva 2002/58/EZ¹⁰, Direktiva 2002/20/EZ¹¹) međusobno se preklapaju, odnose se na istu pravnu oblast i sadrže nejasne definicije. To predstavlja problem sa stanovišta uobičajenih odnosa između korisnika i davaoca usluga, jer prava korisnika neće biti na efektivan i jedinstven način zaštićena, a nedovoljno poznavanje i razumevanje propisa među davaocima usluga može da dovede do smanjenja obima ili potpunog prestanka pružanja usluga korisnicima.¹²

Presuda Evropskog suda pravde (ESP) u slučaju C-101/01, Bodil Lindqvist¹³, u vezi sa zaštitom podataka (prva presuda ove vrste), ima značajne implikacije jer fizičkim licima i privrednim društvima pojašnjava da su podaci o ličnosti zaštićeni i da niko ne može da ih koristi bez prethodnog odobrenja. To je bilo korisno upozorenje ESP onima koji žele da koriste, rukuju i pristupaju podacima bez prava da to čine,

⁸ D. Manolescu, Data protection as a fundamental right, op. cit.

⁹ Direktiva 95/46/EZ.

¹⁰ Direktiva 2002/58/EZ Evropskog parlamenta i Saveta, od 12. jula 2002, o obradi podataka o ličnosti i zaštiti privatnosti u sektoru elektronskih komunikacija (Direktiva o privatnosti u elektronskim komunikacijama), SL list br. L 201, 31. jul 2002, str. 0037–0047 (Direktiva 2002/58/EZ).

¹¹ Direktiva 2002/20/EZ Evropskog parlamenta i Saveta, od 7. marta 2002, o odobrenju elektronskih komunikacionih mreža i usluga (Direktiva o odobrenju), SL list br. L 108, 24. april 2002, str. 0021–0032.

¹² D. Manolescu, Data protection as a fundamental right, op. cit.

¹³ SPEU, krivični postupak protiv Bodil Lindqvist (C-101/01), ECLI:EU:C:2003:596, 6. novembar 2003.

odnosno bez saglasnosti. Od tada sve više zemalja EU pravilno primenjuje Direktivu 95/46/EZ. Presuda takođe može da se tumači i kao pojašnjenje dato onim zemljama koje nisu razumele smisao Direktive 95/46/EZ: podaci su zaštićeni ne samo sa stanovišta privatnosti, već i kao individualno osnovno pravo.¹⁴

Presuđujući u ovom predmetu, ESP je takođe pokušao da uspostavi pravičnu ravnotežu između osnovnih prava i osnovnih sloboda (prava na zaštitu podataka i slobode izražavanja). Kada se radi o ovim osetljivim pitanjima, uvek je teško doneti odluku u korist osnovnih prava, a na štetu osnovnih sloboda ili obratno. Vrlo je teško uspostaviti odgovarajuću ravnotežu prilikom donošenja odluke o tim pitanjima. Nije moguće kategorički priznati jedno osnovno pravo ispred drugog. U ovom slučaju, ljudsko pravo na zaštitu podataka je, prema mišljenju ESP, odnelo prevagu nad ljudskim pravom na slobodu izražavanja, budući da nečije privatne informacije imaju istu vrednost kao i nečije pravo na izražavanje sopstvenih uverenja kada to lice bez pristanka koristi privatne podatke trećeg lica. U ovom slučaju je ESP utvrdio da nije dozvoljeno kršenje osnovnih sloboda, kao što je zaštita podataka, radi izražavanja ličnih uverenja.¹⁵

Sudska praksa Evropskog suda za ljudska prava

Evropski sud za ljudska prava (ESLP) je odlučivao o obavezi zemalja da štite pravo pojedinca od preteranog zadiranja državnih organa tokom istrage u okviru krivičnog postupka, konkretno u vezi sa praćenjem korespondencije i prisluškivanjem telefonskih razgovora. Tako je, na primer, u predmetu *Klass et al. v. Germany*¹⁶ Sud zauzeo stav da tajni nadzor ne predstavlja kršenje prava na privatnost i korespondenciju, budući da su postupci nadzora dovoljno detaljno i rigorozno propisani. ESLP je zaključio da je potreba da

¹⁴ D. Manolescu, Data protection as a fundamental right, op. cit.

¹⁵ D. Manolescu, Data protection as a fundamental right, op. cit.

¹⁶ ECHR, *Klass et al. v. Germany*, br. 5029/71, 6. septembar 1978.

se zaštititi bezbednost države i spreče neredi ili izvršenje krivičnog dela radnja koja je neophodna u demokratskom društvu. Nasuprot tome, ESLJP je presudio drugačije u predmetu *Malone v. the United Kingdom*¹⁷, u kojem je odlučivano o dozvoljenosti policijskog prisluškivanja telefonskih razgovora i vođenja „registra“ telefonskih brojeva pozvanih s određenog pretplatničkog broja. U tom slučaju je utvrđeno da je došlo do kršenja prava na privatnost, budući da je mogućnost prisluškivanja telefonskih razgovora u Ujedinjenom Kraljevstvu uređena preterano proizvoljno. U vezi s listom pozvanih telefonskih brojeva, ESLJP je ocenio da je ta radnja zakonita i uobičajena u poslovnom svetu, ali da prenos tih podataka policiji predstavlja neosnovano zadiranje u pravo na privatnost, jer nije postojao nikakav zakonski osnov, niti pristanak dotičnih lica.¹⁸

Predmet *Sciacca v. Italy*¹⁹ odnosi se na objavljivanje fotografije lica u krivičnom postupku. U pitanju je bila sumnja na izvršenje krivičnog dela od strane više lica, koja su se teretila za ucenu, prevaru i falsifikovanje u jednoj privatnoj školi na Siciliji. Među njima je bio i jedan nastavnik, koji je prijavljen finansijskoj policiji i kasnije držan u kućnom pritvoru. Policija je tom prilikom napravila njegovu fotografiju i uzela otiske prstiju. Javni tužilac je na konferenciji za štampu podelio fotografiju novinarima, koji su je objavili u više dnevnih novina. Iako je osumnjičenom kasnije izrečena zatvorska i novčana kazna, utvrđeno je da objavljivanje fotografije predstavlja zadiranje u privatnost. Pošto tužilac nije dobio zadovoljenje u pravosudnom sistemu Italije, o predmetu je odlučivao ESLJP, koji je presudio da je objavljivanje predstavljalo kršenje prava na privatnost, s obzirom na to da isto nije bilo neophodno, a nije bilo ni dozvoljeno, pošto je policija fotografiju napravila za druge svrhe.²⁰

¹⁷ ECHR, *Malone v. the United Kingdom*, br. 8691/79, 26. april 1985.

¹⁸ Poverenik za informacije Slovenije, Smernice: Mediji i zaštita podataka o ličnosti, dostupno na adresi: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Media_and_the_Protection_of_Personal_Data.pdf (pristupljeno 20. 3. 2017).

¹⁹ ECHR, *Sciacca v. Italy*, br. 50774/99, 11. januar 2005.

²⁰ Smernice Poverenika za informacije Slovenije: Mediji i zaštita podataka o ličnosti, nav. delo.

U predmetu *Uzun v. Germany*²¹, tužilac i još jedan čovek su stavljeni pod prismotru putem uređaja sistema za globalno pozicioniranje (GPS) koji je bio postavljen na automobil tog drugog čoveka zbog sumnje da su učestvovali u bombaškim napadima. ESLJP je u ovom slučaju zauzeo stanovište da posmatranje tužioca putem GPS-a predstavlja zadiranje u njegov privatni život, koji štiti Član 8. EKLJP. Međutim, nadzor putem GPS-a je vršen u skladu sa zakonom i bio je srazmeran legitimnom cilju istrage nekoliko tačaka optužnice za pokušaj ubistva, pa je stoga bio neophodan u demokratskom društvu. Sud je zaključio da nije došlo do kršenja Člana 8. EKLJP.²²

Ne samo da su prava i obaveze države ograničeni kada njeni organi zadiru u prava pojedinaca i kada moraju da poštuju mere (negativne obaveze), već je ona takođe dužna da usvoji pozitivne mere i obezbedi adekvatnu sudsku zaštitu lica od drugih lica. Tako je ESLJP doneo presudu o zloupotrebi interneta pre usvajanja preporuka Evropske komisije (EK), rezolucija Ujedinjenih nacija i Direktive Evropske unije 2006/24/EZ²³, koja menja i dopunjuje Direktivu 2002/58/EZ. Direktivom EU 2006/24/EZ propisana je obaveza država da usvoje protivmere u slučaju visokotehnološkog kriminala. U uporednoj studiji²⁴, koju je ESLJP izvršio u jednom slučaju, utvrđeno je da su mnoge zemlje propisale obavezu pružalaca telekomunikacionih usluga da dostave računarske podatke (uključujući i podatke o pretplatnicima), nezavisno od prirode krivičnog dela. Posledično, Sud je usvojio žalbu oca dvanaestogodišnjeg dečaka u predmetu *K.U. v. Finland*²⁵, pošto ni Prvostepeni ni Apelacioni sud nisu zaštitili

²¹ ECHR, *Uzun v. Germany*, br. 35623/05, 2. septembar 2010.

²² Smernice Poverenika za informacije Slovenije: Mediji i zaštita podataka o ličnosti, nav. delo.

²³ Direktiva 2006/24/EZ Evropskog parlamenta i Saveta, od 15. marta 2006, o zadržavanju podataka dobijenih ili obrađenih u vezi sa pružanjem javno dostupnih elektronskih komunikacionih usluga ili javnih komunikacionih mera i o izmeni Direktive 2002/58/EZ, SL list br. L 105, 13. 4. 2006, str. 54–63.

²⁴ *Comparative Law in the Reasoning of the ECHR*, dostupno na adresi: http://epubs.surrey.ac.uk/186004/3/Microsoft_Word_-_Working_draft_comparative_law.pdf (pristupljeno 17. 3. 2017).

²⁵ ECHR, *K.U. v. Finland*, br. 2872/02, 2. decembar 2008.

psihološke i moralne interese pojedinca (posebno adolescenta ili ugrožene osobe) koji je postao meta pedofila. U tom slučaju, neko je počinio krivično delo time što je na internetu objavio oglas kojim dvanaestogodišnji dečak traži intiman kontakt sa dečakom iste visine ili višim od njega, koji bi mu „objasnio šta treba da radi“. Lice je detaljno navelo podatke o ličnosti adolescenta, uključujući i datum rođenja i njegov fizički opis, i stavilo link ka njegovoj internet stranici koja je sadržala njegovu fotografiju, adresu elektronske pošte i broj telefona. Sud je državi naložio da preduzme protivmere i osigura konkretne i efikasne mere kako bi utvrdila identitet lica koje je objavilo oglas i tako omogućila njegovo krivično gonjenje.²⁶

Što se tiče pristupa podacima o ličnosti državnih službenika, treba istaći da, u skladu s doktrinom očekivane privatnosti – koju je ESLJP prihvatio u predmetima *Halford v. United Kingdom*²⁷ i *Copland v. United Kingdom*²⁸ – državni službenici ne mogu da očekuju privatnost u pogledu svog imena, zvanja, radnog mesta, zarade, adrese mesta rada i onih delova uspešne prijave na konkurs za radno mesto u kojima se navode kvalifikacije kandidata vezane za obavljanje konkretnog posla.²⁹

²⁶ Smernice Poverenika za informacije Slovenije: Mediji i zaštita podataka o ličnosti, nav. delo.

²⁷ ECHR, *Halford v. United Kingdom*, 25. jun 1997, Izveštaji 1997-III.

²⁸ ECHR, *Copland v. United Kingdom*, br. 62617/00, 3. april 2007.

²⁹ Smernice Poverenika za informacije Slovenije: Mediji i zaštita podataka o ličnosti, nav. delo.

1.1. POVELJA EU O OSNOVNIM PRAVIMA

Povelja o osnovnim pravima propisuje osnovna prava koja moraju da poštuju EU i države članice prilikom primene prava EU. To je pravno obavezujući akt izrađen da bi se izričito priznala uloga osnovnih prava u pravnom poretku EU i da bi ova prava postala vidljiva.³⁰

Povelju o osnovnim pravima zvanično su proglasili Parlament, Savet i Komisija u Nici 2000. godine. Nakon izmena, ponovo je proglašena 2007. godine. Međutim, zvanično proglašavanje nije učinilo Povelju pravno obavezujućom. Usvajanje nacrtu Ustava za Evropu, potpisanog 2004. godine, dalo bi joj obavezujuću snagu. Neuspešan proces ratifikacije značio je da Povelja ostaje samo proglašenje prava do usvajanja Lisabonskog ugovora.

Povelja je postala pravno obavezujuća 1. decembra 2009. godine. Član 6(1) Ugovora o EU sada propisuje da „Unija priznaje prava, slobode i principe propisane Poveljom o osnovnim pravima Evropske unije [...], koja ima istu pravnu vrednost kao i ugovori“. Dakle, Povelja predstavlja primarno zakonodavstvo EU; kao takva, služi kao parametar za ispitivanje valjanosti podzakonskih akata EU i nacionalnih mera.³¹

Povelja utvrđuje:

- sva prava koja se nalaze u sudskoj praksi Suda pravde EU;
- prava i slobode koji su zagarantovani Evropskom konvencijom o ljudskim pravima;
- druga prava i principe proistekle iz zajedničkih ustavnih tradicija država članica EU i drugih međunarodnih akata.

³⁰ http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU_1.1.6.html (pristupljeno 20. 3. 2017).

³¹ Isto.

Sadržaj

Povelja o osnovnim pravima je podeljena u sedam naslova, od kojih je šest posvećeno nabravanju konkretnih vrsta prava, a u poslednjem je pojašnjena oblast primene Povelje i principi kojima se uređuje njeno tumačenje. Jedna značajna karakteristika Povelje je inovativno grupisanje prava, čime je napušteno tradicionalno pravljenje razlike između građanskih i političkih prava, s jedne strane, i ekonomskih i socijalnih prava, s druge. Istovremeno, u Povelji se pravi jasna razlika između prava i principa. Potonji, prema Članu 52(5), treba da se sprovedu kroz dodatno zakonodavstvo i postaju značajni za sudove samo u slučajevima koji uključuju tumačenje i zakonitost takvih zakona.

Suštinski deo Povelje podeljen je na sledeći način:

Naslov I („Dostojanstvo“) podržava pravo na ljudsko dostojanstvo, život i integritet lica i potvrđuje zabranu mučenja i ropstva.

Naslov II („Slobode“) podržava pravo na slobodu i poštovanje privatnog i porodičnog života, pravo na zaštitu podataka o ličnosti, pravo na sklapanje braka i zasnivanje porodice i pravo na slobodu mišljenja, savesti i veroispovesti, izražavanja i okupljanja. Takođe potvrđuje pravo na obrazovanje, rad, imovinu i azil.

Naslov III („Jednakost“) potvrđuje princip jednakosti i zabrane diskriminacije, kao i poštovanje kulturne, verske i jezičke raznolikosti. Takođe garantuje posebnu zaštitu za prava deteta, starih lica i osoba sa invaliditetom.

Naslov IV („Solidarnost“) obezbeđuje zaštitu prava radnika, uključujući i pravo na kolektivno pregovaranje i delovanje i pravične i poštene uslove rada. Takođe priznaje dodatna prava i principe, poput prava na socijalno osiguranje, prava na pristup zdravstvenoj zaštiti i principa zaštite životne sredine i zaštite potrošača.

Naslov V („Prava građana“) nabraja prava građana Unije: pravo da se bira i da se bude biran na izborima za Evropski parlament i na opštinskim izborima, pravo na dobru upravu i pravo na peticiju, pravo na pristup dokumentima, na diplomatsku zaštitu i slobodu kretanja i nastanjivanja.

Naslov VI („Pravda“) potvrđuje pravo na delotvorno pravno sredstvo i pravično suđenje, pravo na odbranu, načela zakonitosti i srazmernosti krivičnih dela i pravo da se nekome ne može suditi ili izricati kazna u krivičnom postupku dva puta za isto krivično delo.³²

Iako Povelja uglavnom ponovo potvrđuje prava koja već postoje u državama članicama i koja su priznata kao sastavni deo opštih principa prava EU, ona je takođe inovativna po nekim pitanjima. Na primer, invaliditet, starost i seksualna orijentacija se sada eksplicitno navode kao zabranjene osnove za diskriminaciju. Pored toga, Povelja obuhvata neka „moderna“ prava, što se vidi u primeru zabrane reproduktivnog kloniranja ljudskih bića.

Međutim, osnovna vrednost Povelje nije u njenom inovativnom karakteru, već u eksplicitnom priznavanju ključne uloge tih osnovnih prava u pravnom poretku EU. Dakle, Poveljom se izričito potvrđuje da je EU zajednica prava i vrednosti i da se osnovna prava građana nalaze u srcu EU.³³

Oblast primene i tumačenje

Naslov VII Povelje obuhvata neke opšte odredbe kojima se uređuje njeno tumačenje i primena. Domašaj Povelje u odnosu na lica na koja se primenjuje potencijalno je veoma širok: većina prava koje priznaje garantuju se „svakome“, bez obzira na državljanstvo ili

³² http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU_1.1.6.html (pristupljeno 20. 3. 2017).

³³ http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU_1.1.6.html (pristupljeno 23. 2. 2017).

status. Međutim, neka prava se garantuju samo građanima (većina prava navedenih pod Naslovom V), dok su druga od posebnog značaja za lica koja nisu državljani EU (na primer, pravo na azil) ili za posebne kategorije lica (kao što su radnici).³⁴

Materijalna oblast primene Povelje izričito je definisana u Članu 51, u kojem se navodi da se njene odredbe odnose samo na institucije i tela EU i na države članice kada sprovode pravo EU. Ova odredba služi da se povuče granica između oblasti primene Povelje i oblasti primene nacionalnih ustava: Povelja ne obavezuje države članice ako ne sprovode pravo EU. Međutim, Poveljom se ne proširuju ovlašćenja ili nadležnosti Unije, čime se obezbeđuje da usvajanje Povelje samo po sebi ne povećava nadležnosti Unije na štetu nadležnosti država članica.

Dodatna pravila kojima se potvrđuje značaj nacionalnih ustavnih tradicija i nacionalnih zakona nalaze se u Članovima 52. i 53. Prvi od ovih članova propisuje da se osnovna prava moraju tumačiti u skladu sa ustavnim tradicijama koje su zajedničke svim državama članicama, kao i EKLJP, i uzimajuću u potpunosti u obzir nacionalne zakone i prakse. U Članu 53. se jasno navodi da Povelja ne može da ograniči ili negativno utiče na nivo zaštite osnovnih prava koji je već obezbeđen pravom Unije, međunarodnim pravom (EKLJP) i ustavima država članica.³⁵

Iako Povelja obuhvata nekoliko prava, ne garantuje se njihova neograničena zaštita. Štaviše, Članom 52. odobravaju se ograničenja za ostvarivanje prava, ako su propisana zakonom, poštuju suštinu prava koje je u pitanju i ako su srazmerna i neophodna za zaštitu prava drugih ili opšteg interesa. Pored toga, dok su neka prava definisana kao apsolutna, druga su garantovana samo „u skladu sa pravom

³⁴ http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU_1.1.6.html (pristupljeno 23. 2. 2017).

³⁵ Ibid.

Unije i nacionalnim zakonima i praksama“, što znači da na obuhvat tih prava mogu da se primenjuju dodatna ograničenja.

Povelja se podjednako primenjuje u svim državama članicama EU. Iako je usvojen Protokol da bi se pojasnila njena primena u Ujedinjenom Kraljevstvu i Poljskoj, njime se ne ograničava niti isključuje njen uticaj na pravne poretke ove dve države članice, kako je izričito priznao Sud pravde³⁶.

Povelja se, na primer, primenjuje kada države članice EU usvoje ili primenjuju nacionalni zakon o sprovođenju direktive EU ili kada njihovi organi neposredno primenjuju uredbu EU. U slučajevima kada se Povelja ne primenjuje, zaštita osnovnih prava je zagarantovana ustavima ili ustavnim tradicijama država članica EU i međunarodnim konvencijama koje su ratifikovale. Poveljom se ne proširuje nadležnost EU na pitanja koja nisu uključena u ugovore u okviru njene nadležnosti.³⁷

Zaštita podataka o ličnosti

Članom 8. Povelje obezbeđena je zaštita podataka o ličnosti:

- 1. Svako ima pravo na zaštitu svojih podataka o ličnosti.*
- 2. Takvi podaci moraju da se obrađuju pošteno, u određene svrhe i na osnovu pristanka lica na koje se podaci odnose ili na drugoj legitimnoj osnovi koja je propisana zakonom. Svako ima pravo na pristup podacima koji su prikupljeni o njemu i pravo da zatraži njihovu ispravku.*
- 3. Poštovanje ovih pravila pod kontrolom je nezavisnog organa.*

Ovaj član je zasnovan na Članu 286. Ugovora o osnivanju Evropske zajednice i Direktivi 95/46/EZ, kao i na Članu 8. EKLJP i na Kon-

³⁶ CJEU, N. S. (C-411/10) v Secretary of State for the Home Department and M. E. (C-493/10), A. S. M., M. T., K. P., E. H. v Refugee Applications Commissioner, Minister for Justice, Equality and Law Reform, ECLI:EU:C:2011:865, 21. decembar 2011.

³⁷ http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU_1.1.6.html (pristupljeno 23. 2. 2017).

venciji Saveta Evrope od 28. januara 1981. o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti, koju su ratifikovale sve države članice. Član 286. Ugovora o EZ sada je zamenjen Članom 16. Ugovora o funkcionisanju Evropske unije i Članom 39. Ugovora o Evropskoj uniji. Takođe se upućuje na Uredbu (EZ) br. 45/2001 Evropskog parlamenta i Saveta o zaštiti lica u vezi sa obradom podataka o ličnosti u institucijama i telima Zajednice i slobodnom kretanju takvih podataka (SL list br. L 8, 12. 1. 2001, str. 1). Navedena direktiva i uredba sadrže uslove i ograničenja za ostvarivanje prava na zaštitu podataka o ličnosti.

1.2. DIREKTIVA 95/46/EZ

Direktiva 95/46/EZ Evropskog parlamenta i Saveta, od 24. oktobra 1995, o zaštiti lica u vezi sa obradom podataka o ličnosti i slobodnom kretanju takvih podataka³⁸ je referentni tekst na nivou Evrope o zaštiti podataka o ličnosti. Njom se uspostavlja regulatorni okvir čiji je cilj uspostavljanje ravnoteže između visokog nivoa zaštite privatnosti lica i slobodnog kretanja podataka o ličnosti unutar EU. Da bi se to postiglo, Direktiva propisuje stroga ograničenja za prikupljanje i korišćenje podataka o ličnosti i zahteva da svaka država članica osnuje nezavisno nacionalno telo odgovorno za nadzor nad svim aktivnostima povezanim sa obradom podataka o ličnosti. Direktiva 95/46/EZ stupila je na snagu 13. decembra 1995. godine, a rok za transponovanje u državama članicama bio je 24. oktobar 1998. Direktiva će biti stavljena van snage Opštom uredbom o zaštiti podataka (OUZP)³⁹, koja će stupiti na snagu u maju 2018. godine.

Sadržaj

Ova direktiva se primenjuje na podatke koji se obrađuju automatski (npr. računarska baza podataka klijenata) i podatke sadržane u sistemima za arhiviranje koji nisu automatski ili namenjeni da budu deo takvih sistema (tradicionalni dosijei na papiru).

Ova direktiva se ne primenjuje na obradu podataka:

- od strane fizičkog lica prilikom aktivnosti isključivo lične prirode ili aktivnosti vezane za domaćinstvo;

³⁸ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046> (pristupljeno 2. 3. 2017).

³⁹ Uredba (EU) 2016/679 Evropskog parlamenta i Saveta, od 27. aprila 2016, o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i slobodnom kretanju takvih podataka, kojom se stavlja van snage Direktiva 95/46/EZ (Opšta uredba o zaštiti podataka), SL list br. L 119, 4. 5. 2016, str. 1–88.

- u toku aktivnosti koja ne spada u oblast primene prava Zajednice, kao što su aktivnosti koje se tiču javne bezbednosti, odbrane ili državne bezbednosti.

Cilj Direktive je da zaštiti prava i slobode lica u vezi sa obradom podataka o ličnosti tako što propisuje ključne kriterijume za zakonitost obrade i načela kvaliteta podataka.⁴⁰

Obrada podataka je zakonita samo ako:

- je lice na koje se podaci odnose nedvosmisleno dalo svoj pristanak; ili
- je obrada podataka neophodna za realizaciju ugovora u kojem je lice na koje se podaci odnose ugovorna strana; ili
- je obrada neophodna za ispunjavanje zakonske obaveze rukovaoca podataka; ili
- je obrada neophodna da bi se zaštitili životni interesi lica na koje se podaci odnose; ili
- je obrada neophodna za izvršenje zadatka koji se obavlja u javnom interesu ili za vršenje zvaničnog ovlašćenja koje je dato rukovaocu podataka ili trećem licu; ili
- je obrada neophodna za potrebe legitimnog interesa rukovaoca podataka ili trećeg lica, osim u slučaju da nad takvim interesima preovlađuju interesi osnovnih prava i sloboda lica na koje se podaci odnose koji zahtevaju zaštitu.

Načela kvaliteta podataka, koja moraju da budu primenjena na sve zakonite radnje obrade podataka, su:

- podaci o ličnosti moraju da se obrađuju pravično i zakonito i da se prikupljaju u određene, izričite opravdane svrhe. Takođe moraju da budu primereni i relevantni i ne smeju da budu preterani, moraju da budu tačni i, prema potrebi, ažurni, ne smeju da

⁴⁰ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046> (pristupljeno 2. 3. 2017).

se čuvaju duže nego što je neophodno i mogu da se obrađuju isključivo u svrhe u koje su prikupljeni;

- posebne kategorije obrade: zabranjeno je obrađivati podatke o ličnosti koji otkrivaju rasno ili etničko poreklo, političke stavove, verska ili filozofska uverenja, članstvo u sindikatima, kao i obrađivati podatke o zdravstvenom stanju ili seksualnom životu. Ova odredba sadrži određene rezerve u vezi sa npr. slučajevima kada je obrada neophodna radi zaštite životnih interesa lica na koje se podaci odnose ili za potrebe preventivne medicine ili medicinske dijagnoze.⁴¹

Lice čiji se podaci obrađuju, odnosno lice na koje se podaci odnose, može da ostvari sledeća prava:

- pravo na dobijanje informacija: rukovalac podataka mora da pruži licu na koje se podaci odnose i od kojeg su podaci prikupljeni određene informacije koje se odnose na njega (identitet rukovaoca podataka, svrhe obrade, primaoci podataka itd.);
- pravo lica na koje se podaci odnose na pristup podacima: svako lice na koje se podaci odnose treba da ima pravo da ih dobije od rukovaoca podataka;
- pravo da uloži prigovor na obradu podataka: lice na koje se podaci odnose treba da ima pravo da uloži prigovor, na zakonskim osnovama, na obradu njegovih podataka. Lice na koje se podaci odnose takođe treba da ima pravo da uloži prigovor, na zahtev i besplatno, na obradu podataka o ličnosti za koje rukovalac podataka pretpostavlja da se obrađuju u svrhe direktnog marketinga. Konačno, lice na koje se podaci odnose treba da bude obavešteno pre otkrivanja podataka o ličnosti trećim licima za potrebe direktnog marketinga i mora izričito da mu se ponudi pravo da uloži prigovor na takvo otkrivanje.

⁴¹ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046> (pristupljeno 2. 3. 2017).

Drugi relevantni aspekti za obradu podataka:

- izuzeća i ograničenja za prava lica na koje se podaci odnose: obuhvat principa koji se odnose na kvalitet podataka, informacije koje se daju licu na koje se podaci odnose, pravo na pristup i objavljivanje obrade mogu da budu ograničeni da bi se zaštitili aspekti kao što su bezbednost države, odbrana, javna bezbednost, gonjenje učinilaca krivičnih dela, bitan ekonomski ili finansijski interes države članice ili Evropske unije ili zaštita lica na koje se podaci odnose;
- poverljivost i bezbednost obrade: nijedno lice koje odgovara rukovaocu podataka ili obrađivaču, uključujući i samog obrađivača, koje ima pristup podacima o ličnosti, ne sme da ih obrađuje bez naloga rukovaoca. Pored toga, rukovalac podataka mora da primeni odgovarajuće mere kako bi zaštitio podatke o ličnosti od slučajnog ili nezakonitog uništenja, izmene, neovlašćenog otkrivanja ili pristupa;
- obaveštavanje nadzornog organa o obradi: rukovalac mora da obavesti nadzorni organ pre početka vršenja bilo kakvih radnji obrade. Nadzorni organ nakon prijema obaveštenja vrši prethodne provere da bi se odredili posebni rizici za prava i slobode lica na koje se podaci odnose. Moraju se preduzimati mere da bi se obezbedilo da postupci obrade budu objavljeni, a nadzorni organi moraju da vode registar postupaka obrade o kojima je dostavljeno obaveštenje.

Svako lice ima pravo na pravno sredstvo za svako kršenje prava koja su mu garantovana nacionalnim zakonodavstvom koje se primenjuje na predmetnu obradu. Pored toga, svako lice koje je pretrpelo štetu kao posledicu nezakonite obrade njegovih podataka o ličnosti ima pravo na odštetu za pretrpljenu štetu.⁴²

Prenos podataka iz države članice u treću zemlju sa adekvatnim nivoom zaštite je dozvoljen. Međutim, iako se prenos podataka ne

⁴² <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046> (pristupljeno 2. 3. 2017).

vrši ako nije zagarantovan adekvatan nivo zaštite, u Direktivi je navedeno nekoliko izuzetaka od ovog pravila, npr. ako je lice na koje se podaci odnose dalo saglasnost za prenos, u slučaju zaključenja ugovora, ako je prenos podataka neophodan na osnovu javnog interesa, ali i ako država članica odobri Obavezujuća korporativna pravila ili standardne ugovorne klauzule.

Cilj direktive je da podstiče sastavljanje nacionalnih kodeksa ponašanja i kodeksa ponašanja Zajednice koji treba da doprinesu pravilnom sprovođenju nacionalnih propisa i propisa Zajednice.

Svaka država članica propisuje jedan ili više nezavisnih državnih organa odgovornih za praćenje primene propisa koje usvoji država članica u skladu sa Direktivom na njihovim teritorijama.⁴³

⁴³ <http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046> (pristupljeno 2. 3. 2017).

1.3. OPŠTA UREDBA O ZAŠTITI PODATAKA

Opšta uredba o zaštiti podataka (OUZP) (Uredba (EU) 2016/679) je uredba kojom Evropski parlament, Evropski savet i Evropska komisija nameravaju da ojačaju i objedine zaštitu podataka za fizička lica u EU. Takođe se bavi i iznošenjem podataka o ličnosti izvan EU. Glavni ciljevi OUZP su da se građanima vrati kontrola nad njihovim podacima o ličnosti i da se pojednostavi regulatorno okruženje za međunarodno poslovanje usvajanjem jedinstvenog zakonodavstva u EU.⁴⁴ Kada OUZP počne da se primenjuje, zameniće direktivu o zaštiti podataka (zvaničan naziv Direktiva 95/46/EZ)⁴⁵ iz 1995. godine. Neke će možda zbuniti činjenica da, pored nove uredbe, postoji i nova direktiva; ona će se primenjivati na policijske procedure, koje će se i dalje razlikovati među državama članicama.⁴⁶

Uredba je usvojena 27. aprila 2016. godine. Na snagu stupa 25. maja 2018, nakon dvogodišnjeg prelaznog perioda i, za razliku od direktive, ne zahteva donošenje zakonodavstva o njenom sprovođenju od strane nacionalnih vlada.⁴⁷

„Predloženi novi režim zaštite podataka u EU proširuje područje primene zakona o zaštiti podataka u EU na sva strana privredna društva koja obrađuju podatke rezidenata EU. Ona predviđa harmonizaciju propisa o zaštiti podataka u čitavoj EU, što će privrednim društvima sa sedištem izvan EU olakšati poštovanje tih propisa; međutim, cena koju plaćaju za to je poštovanje strogog režima

⁴⁴ Predsedništvo Saveta: „Tekst koji je rezultat kompromisa. Nekoliko delimičnih opštih pristupa je bilo od presudnog značaja za približavanje gledišta Saveta o predlogu Opšte uredbe o zaštiti podataka u celini. Tekst Uredbe koji predsedništvo dostavlja na odobravanje kao opšti pristup nalazi se u prilogu.“ 201 strana, 11. jun 2015, <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>.

⁴⁵ Direktiva 95/46/EZ.

⁴⁶ “European Commission – Fact Sheet. Questions and Answers – Data protection reform”. Evropska komisija. 21. decembar 2015, dostupno na adresi http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (pristupljeno 2. 3. 2017).

⁴⁷ Blackmer, W.S. (5. maj 2016). “GDPR: Getting Ready for the New EU General Data Protection Regulation”. Information Law Group. InfoLawGroup LLP.

zaštite podataka s visokim kaznama, koje se kreću i do 4% prometa koji ostvare u svetu.⁴⁸ Verzija koju je usvojio Parlament predviđala je više kazne, i do 5%.⁴⁹ Nakon pregovora u okviru trijaloga između Evropskog parlamenta, Evropske komisije i Saveta ministara, postignut je opšti konsenzus o tekstu OUZP, kao i o novčanoj kazni od 4% za nepoštovanje obaveza.⁵⁰

Sadržaj

Cilj OUZP je zaštita svih građana EU od povreda privatnosti i zaštite podataka u svetu koji se u sve većoj meri oslanja na podatke i koji se drastično razlikuje od sveta u kojem je doneta direktiva iz 1995. godine. Iako su zadržana ključna načela zaštite podataka iz prethodne direktive, predložene su brojne izmene regulatornih politika.

Uredba se primenjuje ako rukovalac ili obrađivač podataka (organizacija) ili lice na koje se podaci odnose ima poslovno sedište, odnosno prebivalište u EU. Dalje (za razliku od postojeće Direktive), Uredba se takođe primenjuje i na organizacije sa sedištem izvan Evropske unije ako obrađuju podatke o ličnosti rezidenata EU. Uredba se ne primenjuje na obradu podataka o ličnosti za svrhe nacionalne bezbednosti ili gonjenja učinilaca krivičnih dela („nadležni organi u svrhu sprečavanja, istrage, otkrivanja i gonjenja za krivična dela ili izvršenja krivičnih sankcija“). Prema mišljenju Evropske komisije, „podatak o ličnosti je svaka informacija koja se odnosi na pojedinca, nezavisno od

⁴⁸ “New draft European data protection regime”. M law group, dostupno na adresi: http://mlaw-group.de/news/publications/detail.php?we_objectID=227 (pristupljeno 2. 3. 2017).

⁴⁹ Nezvanična prečišćena verzija nakon glasanja Komiteta LIBE koju je podneo izvestilac Jan Filip Albreht, 22. oktobar 2013, dostupno na adresi: <http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf> (pristupljeno 2. 3. 2017).

⁵⁰ Član 83. (5) prve verzije Saveta nakon trijaloga utvrđuje maksimalan iznos novčane kazne na 4% globalnog prometa i 20.000.000 evra, dostupno na adresi: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT (pristupljeno 2. 3. 2017). Komisija je usvojila gledišta iz dokumenta Saveta 11. aprila 2016. godine, COM/2016/214/FINALiST 5419 2016 ADD 1 – 2012/011 (OLP).

toga da li se odnosi na njegov, odnosno njen privatni, profesionalni ili javni život. To može da bude bilo šta – ime, fotografija, adresa elektronske pošte, podaci o bankovnom računu, postovi na društvenim mrežama, podaci o zdravstvenom stanju ili IP adresa računara”.⁵¹

Glavne promene

Proširenje teritorijalnog obuhvata (vanteritorijalna primena)

Možda i najveća promena u regulatornom okruženju privatnosti podataka je proširenje područja primene OUZP, koja se primenjuje na sva privredna društva koja obrađuju podatke o ličnosti lica nastanjenih u Uniji, nezavisno od toga gde se privredno društvo nalazi. Ranije je teritorijalna primena direktive bila nejasno određena, uz pozivanje na obradu podataka „u okviru delatnosti poslovne jedinice“. Ova tema se javila u nekoliko sudskih predmeta koji su privukli veliku pažnju. OUZP vrlo jasno određuje svoje područje primene – primenjuje se na obradu podataka o ličnosti od strane rukovalaca i obrađivača u EU, nezavisno od toga da li se obrada vrši u EU ili ne. OUZP će se takođe primenjivati i na obradu ličnih podataka lica u EU od strane rukovaoca ili obrađivača koji nema sedište u EU ako se aktivnosti odnose na nuđenje proizvoda ili usluga građanima EU (nezavisno od toga da li se zahteva plaćanje) i praćenje ponašanja koje se vrši u EU. Preduzeća izvan EU koja obrađuju podatke građana EU takođe će morati da imenuju predstavnika u EU.⁵²

Kazne

U skladu sa OUZP, organizacijama koje krše odredbe OUZP može biti izrečena novčana kazna u iznosu do 4% godišnjeg globalnog prometa ili 20.000.000 evra (u zavisnosti od toga koji iznos je veći).

⁵¹ Saopštenje za štampu Evropske komisije u kojem su najavljene predložene sveobuhvatne reforme pravila o zaštiti podataka, 25. januar 2012, dostupno na adresi: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (pristupljeno 2. 3. 2017).

⁵² http://ec.europa.eu/justice/data-protection/reform/index_en.htm (pristupljeno 20. 3. 2017).

Ovo je najviši iznos kazne, zaprećen za najteže povrede, npr. nepostojanje adekvatnog pristanka korisnika za obradu podataka ili nepoštovanje osnovnih koncepata „ugrađene privatnosti“. Propisani su različiti iznosi novčanih kazni za različita kršenja odredbi, pa tako, na primer, privrednom društvu može da bude izrečena novčana kazna u visini od 2% za neuredno vođenje evidencija (Član 28), neobaveštavanje nadzornog organa i lica na koje se podaci odnose o povredi ili neobavljanje procene uticaja. Treba naglasiti da se ova pravila primenjuju i na rukovaoce i na obrađivače, što znači da „oblaci“ neće biti izuzeti iz primene OUZP.

Moguće je izricanje sledećih sankcija:

- pisanog upozorenja, u slučaju prvog i nenamernog nepostupanja u skladu s odredbama;
- redovnih periodičnih nadzora nad zaštitom podataka;
- novčane kazne u iznosu do 10.000.000 EUR ili do 2% godišnjeg prometa u svetu za prethodnu finansijsku godinu u slučaju preduzeća, u zavisnosti od toga koji iznos je veći (Član 83, stav 4);
- novčane kazne u iznosu do 20.000.000 EUR ili do 4% godišnjeg prometa u svetu za prethodnu finansijsku godinu u slučaju preduzeća, u zavisnosti od toga koji iznos je veći (Član 83, stavovi 5. i 6).

Pristanak

Valjan pristanak mora da bude dat izričito za prikupljene podatke i za svrhe za koje se podaci koriste (Član 7; definisano u Članu 4). Pristanak za dete⁵³ mora da dâ roditelj ili staratelj deteta, na način koji je moguće proveriti (Član 8). Rukovaoci podataka moraju da budu u stanju da dokažu da je pristanak dat („opt-in“), a pristanak može da bude povučen.⁵⁴

⁵³ Uredba, Član 8 (1): „Za potrebe ove uredbe, u pogledu neposrednog nuđenja usluga informacionog društva detetu, obrada podataka o ličnosti deteta mlađeg od 13 godina je zakonita samo ako je i u meri u kojoj je pristanak dao ili odobrio roditelj ili staratelj deteta“.

⁵⁴ Judy Schmitt, Florian Stahl, How the Proposed EU Data Protection Regulation Is Creating a Ripple Effect Worldwide, 11. oktobar 2012, dostupno na adresi: https://iapp.org/media/presentations/A12_EU_DP_Regulation_PPT.pdf (pristupljeno 2. 3. 2017).

Uvedeni su stroži uslovi vezani za pristanak, a privredna društva više neće moći da koriste dugačke i nerazumljive uslove pružanja usluga pisane pravničkim žargonom, pošto zahtev za pristanak mora da bude dat u razumljivom i lako dostupnom obliku, uz navođenje svrhe obrade podataka u prilogu pristanka. Pristanak mora da bude jasan i odvojen od drugih pitanja i mora biti dat u razumljivom i lako dostupnom obliku, korišćenjem jasnog i jednostavnog jezika. Povlačenje pristanka mora da bude podjednako lako kao i njegovo davanje.

Obaveštenje o povredi zaštite podataka

U skladu sa OUZP, obaveštavanje o povredi zaštite podataka postać će obavezno u svim državama članicama u slučajevima kada povreda može da „prouzrokuje rizik za prava i slobode lica“. To mora da bude učinjeno u roku od 72 sata od saznanja Nadzornog organa o povredi (Član 33). Na prijavljivanje povrede zaštite podataka ne primenjuje se nikakav standard *de minimis*. Obrađivači podataka će takođe imati obavezu da „bez nepotrebnog odlaganja“ obaveste svoje klijente, rukovaoce podataka, odmah po saznanju o povredi zaštite podataka (Član 34).

Pravo pristupa

Deo proširenih prava lica na koja se podaci odnose na osnovu OUZP jeste i pravo lica da od rukovaoce podataka dobiju potvrdu o tome da li se podaci o njima obrađuju, gde se obrada vrši i u koju svrhu. Osim toga, rukovalac je dužan da bez naknade stavi na raspolaganje kopiju podataka o ličnosti u elektronskom formatu. Ova promena predstavlja dramatičan korak u pravcu transparentnosti podataka i osnaživanja lica na koja se podaci odnose.

Pravo na zaborav

Takozvano pravo na zaborav je u verziji OUZP, koju je Evropski parlament usvojio u martu 2014. godine, zamenjeno ograničenijim

pravom na brisanje.⁵⁵ Pravo na zaborav, poznato i kao brisanje podataka, omogućava licu na koje se podaci odnose da od rukovaoca zahteva da obriše njegove podatke o ličnosti, prestane sa daljim slanjem podataka i zaustavi obradu podataka od strane trećih lica u odgovarajućim slučajevima.

Uslovi za brisanje, utvrđeni u Članu 17, podrazumevaju da podaci više nisu relevantni za svrhe za koje se obrada vrši ili da je lice na koje se podaci odnose povuklo pristanak. Takođe treba istaći da ovo pravo od rukovalaca zahteva da, prilikom razmatranja tih zahteva, odmeravaju prava lica u odnosu na „interes javnosti za dostupnosti podataka“. Članom 17. predviđeno je pravo lica na koje se podaci odnose da zahteva brisanje podataka o ličnosti koji se na njega odnose po jednom od niza osnova, uključujući i nepoštovanje Člana 6.1. (zakonitost), koji uključuje slučaj (f) kada interesi ili osnovna prava i slobode lica koja zahtevaju zaštitu podataka o ličnosti prevagnjuju nad legitimnim interesima rukovaoca (videti takođe i *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12).

Prenosivost podataka

OUPZ uvodi prenosivost podataka – pravo lica na koje se podaci odnose da prethodno pružene podatke koji se odnose na njega primi u *uobičajenom i mašinski čitljivom formatu* i ima pravo da iste prenosi drugom rukovaocu.

Pravo na prenosivost podataka predviđeno je Članom 18. OUPZ. Pravni stručnjaci u konačnoj verziji ove mere vide stvaranje „novog prava“ koje „prevazilazi okvire prenosivosti podataka između dva rukovaoca koje je propisano u Članu 18“.⁵⁶

⁵⁵ Baldry, Tony, Hyams, Oliver, “The Right to Be Forgotten”. 1 Essex Court, dostupno na adresi: <https://1essexcourt.wordpress.com/2014/05/15/the-right-to-be-forgotten/> (pristupljeno 2. 3. 2017).

⁵⁶ Cedric Burton, Laura De Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot and Sára G. Hoffman, The Final European Union General Data Protection Regulation, dostupno na adresi: <https://www.bna.com/final-european-union-n57982067329/#!> (pristupljeno 2. 3. 2017).

Ugrađena privatnost

„Ugrađena privatnost“ (engl. *privacy by design*) kao koncept postoji već godinama, ali tek sa OUZP postaje zakonska obaveza. U osnovi, ugrađena privatnost zahteva da zaštita podataka bude ugrađena u same sisteme od početka njihovog projektovanja, umesto da bude samo dodatak. Konkretno – *Rukovalac... primenjuje odgovarajuće tehničke i organizacione mere... na efektivan način... da bi ispunio zahteve sadržane u ovoj uredbi i zaštitio prava lica na koja se podaci odnose*. Član 23. zahteva od rukovalaca da drže i obrađuju samo podatke koji su apsolutno neophodni za obavljanje njegovih poslova (svođenje količine podataka na najmanju moguću meru), uz ograničavanje pristupa podacima o ličnosti na lica koja moraju da vrše obradu.

Ovlašćena lica za zaštitu podataka

Kada obradu vrši organ javne vlasti, osim sudova ili nezavisnih pravosudnih organa koji postupaju u okviru svoje sudske nadležnosti, ili kada u privatnom sektoru obradu vrši rukovalac čija se osnovna delatnost sastoji iz radnji obrade koje zahtevaju redovno i sistematsko masovno praćenje lica na koje se podaci odnose ili masovne obrade posebnih kategorija podataka u skladu sa Članom 9. i podataka o ličnosti koji se odnose na krivičnu i prekršajnu osuđivanost iz Člana 10, rukovaocu ili obrađivaču u praćenju interne usklađenosti s ovom uredbom treba da pomaže lice sa stručnim poznavanjem zakona i prakse u oblasti zaštite podataka. Ovlašćeno lice za zaštitu podataka funkcija je slična ovlašćenom licu za obezbeđivanje usklađenosti poslovanja, ali nije identična, jer se od ovlašćenog lica za zaštitu podataka takođe očekuje da poznaje upravljanje informatičkim procesima, bezbednost podataka (uključujući i postupanje u slučaju kibernetičkog napada) i druga pitanja kontinuiteta poslovanja koja se odnose na čuvanje i obradu podataka o ličnosti i naročito osetljivih podataka. Potrebne veštine obuhvataju više od razumevanja pravne usklađenosti sa zakonima i propisima o zaštiti podataka. Praćenje rada ovlašćenih lica za zaštitu podataka biće u

nadležnosti regulatornog organa, a ne upravnog odbora organizacije u kojoj je ovlašćeno lice zaposleno. Imenovanje ovlašćenog lica za zaštitu podataka u velikoj organizaciji predstavljaće izazov za upravni odbor, ali i za samo lice koje se imenuje. Postoji niz pitanja koja se tiču upravljanja i ljudskog faktora koja će organizacije i privredna društva morati da reše, imajući u vidu obim i prirodu imenovanja. Pored toga, nosilac ove funkcije će morati da formira sopstveni tim za podršku i biće odgovoran za svoje kontinuirano stručno usavršavanje, budući da mora biti nezavisan od organizacije koja ga zapošljava i u osnovi treba da bude „mini regulator“. Funkcija i uloga ovlašćenog lica za zaštitu podataka bliže su određeni 13. decembra 2016. godine donošenjem uputstva.⁵⁷

Rukovaoci trenutno imaju obavezu prijavljivanja radnji obrade podataka lokalnim organima za zaštitu podataka, što može da bude birokratska noćna mora za multinacionalne kompanije, jer većina država članica ima različite zahteve vezane za prijavljivanje. U skladu sa OUZP, neće biti neophodno dostaviti prijavu/registraciju radnji obrade podataka svakom lokalnom organu za zaštitu podataka i neće postojati obaveza obaveštavanja/pribavljanja odobrenja za iznošenje podataka na osnovu Modela ugovornih klauzula (MCC). Umesto toga uvode se zahtevi koji se odnose na vođenje internih evidencija.

Važno je naglasiti da ovlašćeno lice za zaštitu podataka:

- mora da bude imenovano na osnovu profesionalnih kvaliteta i stručnog znanja o zakonu i praksi u oblasti zaštite podataka;
- može da bude zaposlen u organizaciji ili angažovan kao spoljni pružalac usluga;
- mora da dostavi podatke za kontakt nadležnom organu za zaštitu podataka;

⁵⁷ Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), 13. decembar 2016, dostupno na adresi: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf (pristupljeno 2. 3. 2017).

- mora da ima na raspolaganju adekvatne resurse za obavljanje svojih zadataka i održavanje svog stručnog znanja;
- mora da odgovara direktno najvišem nivou rukovodstva;
- ne sme da obavlja nikakve druge zadatke koji bi mogli da dovedu do sukoba interesa.⁵⁸

Jedinstveni skup pravila i jednošalterski sistem

Na sve države članice EU primenjivaće se jedinstven skup pravila. Svaka država članica će formirati nezavisni nadzorni organ koji će postupati po pritužbama i istraživati ih, sankcionisati upravne presteupe itd. Nadzorni organ svake države članice će sarađivati s nadzornim organima drugih država članica, uz pružanje međusobne pomoći i organizovanje zajedničkih poslova. Ako preduzeće ima više poslovnih jedinica u EU, imaće jedan nadzorni organ kao „vodeći organ“, koji se određuje prema „glavnom mestu poslovanja“ (tj. mestu gde se vrše glavne aktivnosti obrade). Vodeći organ će služiti kao „jednošalterski sistem“ za nadzor nad svim aktivnostima obrade koje to preduzeće vrši u čitavoj EU⁵⁹ (Članovi 46-55. OUZP). Rad nadzornih organa koordinisaće Evropski odbor za zaštitu podataka (EDPB). EDPB će zameniti Radnu grupu „Član 29“.

Predviđeni su izuzeci za podatke koji se obrađuju u kontekstu za-
pošljavanja i podatke koji se obrađuju za svrhe nacionalne bezbed-
nosti, na koje i dalje mogu da se primenjuju propisi pojedinačnih
zemalja (Članovi 2(2) (a) i 82. OUZP).

Odgovornost i polaganje računa

Zahtevi koji se odnose na obaveštavanje zadržani su i prošireni. Oni moraju da obuhvataju vreme zadržavanja podataka o ličnosti, a obavezno je dostavljanje informacija za kontakt rukovoca podataka i ovlašćenog lica za zaštitu podataka.

⁵⁸ <http://www.eugdpr.org/key-changes.html> (pristupljeno 2. 3. 2017).

⁵⁹ The Proposed EU General Data Protection Regulation. A guide for in-house lawyers, Hunton & Williams LLP, jun 2015, str. 14.

Moguće je osporiti automatsko donošenje pojedinačnih odluka, uključujući i profilisanje (Član 22). Građani sada imaju pravo da ospore i da se bore protiv odluka koje utiču na njih, a donete su isključivo na osnovu algoritma.

Ugrađena i podrazumevana privatnost (Član 25) podrazumeva da je zaštita podataka ugrađena u poslovne procese za proizvode i usluge prilikom njihovog projektovanja. Podešavanja privatnosti moraju automatski da budu podešena na visok nivo.

Procena uticaja u vezi sa zaštitom podataka (Član 35) obavezno se vrši kada se jave konkretni rizici za prava i slobode lica na koja se podaci odnose. U slučaju visokog rizika zahteva se procena i ublažavanje rizika, kao i prethodno odobrenje organa za zaštitu podataka.

Diskusija i izazovi

Predlog nove uredbe bio je povod za brojne diskusije i kontroverze. Predloženo je na hiljade izmena. Svrha jedinstvenog skupa pravila i ukidanja administrativnih zahteva bila je ušteda novca. Ali kritičari su ukazali na sledeće probleme:

- Obaveza imenovanja ovlašćenog lica za zaštitu podataka je nova obaveza u mnogim zemljama EU i neki su je kritikovali zbog administrativnog opterećenja koje podrazumeva.
- Prilikom izrade OUZP, u središtu pažnje bile su društvene mreže i davaoci usluga računarstva u oblaku, ali nisu u dovoljnoj meri uzeti u obzir zahtevi koji se odnose na rukovanje podacima o zaposlenima.⁶⁰
- Prenosivost podataka se ne smatra ključnim aspektom zaštite podataka, već funkcionalnim zahtevom za društvene mreže i davaoce usluga računarstva u oblaku.

⁶⁰ Regina Mühlich, Expert tips: Get your business ready for OUZP, dostupno na adresi: <https://tresorit.com/blog/expert-tips-business-gdpr-ready/> (pristupljeno 2. 3. 2017).

- Jezički kadrovski izazovi za organe za zaštitu podataka (DPA):
 - o neevropska privredna društva će se verovatno odlučiti za organ za zaštitu podataka Irske zbog engleskog jezika. To će zahtevati angažovanje velikih resursa u tim zemljama;
 - o građani EU više nemaju jedan organ za zaštitu podataka kojem mogu da se obrate sa svojim problemima, već moraju da sarađuju sa organom za zaštitu podataka koji izabere konkretno privredno društvo. Mogu se očekivati problemi u komunikaciji zbog stranih jezika.
- Nova uredba je u nesaglasnosti sa drugim neevropskom zakonima i propisima i praksom (npr. nadzor od strane vlada). Privredna društva iz tih zemalja se više ne mogu smatrati prihvatljivima za obradu podataka o ličnosti iz EU. Videti deo o sporazumu Privacy Shield između EU i SAD.
- Najveći izazov može da bude sprovođenje OUZP u praksi:
 - o za sprovođenje OUZP EU biće potrebne sveobuhvatne promene poslovne prakse u privrednim društvima koja nisu uvela uporediv nivo privatnosti pre stupanja uredbe na snagu (a posebno u neevropskim društvima koja rukuju ličnim podacima iz EU);
 - o već se zapaža nedostatak eksperata za privatnost i znanja o privatnosti, a novi zahtevi bi mogli dodatno da pogoršaju situaciju. Stoga će edukacija o zaštiti podataka i privatnosti biti kritičan faktor za uspeh OUZP;
 - o Evropska komisija i organi za zaštitu podataka moraju da obezbede dovoljne resurse i ovlašćenja za sprovođenje i svi evropski organi za zaštitu podataka moraju da se dogovore o jedinstvenom nivou zaštite podataka, jer različita tumačenja Uredbe svejedno mogu da dovedu do različitih nivoa privatnosti;
 - o Evropska politika međunarodne trgovine još uvek nije u skladu sa OUZP.⁶¹

⁶¹ Kristina Irion, Svetlana Yakovleva, and Marija Bartl, Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements, Institute for Information Law (IViR), University of Amsterdam, 22. septembar 2016.

ZAŠTITA PODATAKA I NADLEŽNOSTI INSTITUCIJA EVROPSKE UNIJE



2.1. EVROPSKA KOMISIJA

Evropska komisija (EK) je institucija EU odgovorna za predlaganje zakonodavstva, sprovođenje odluka, potvrđivanje ugovora EU i rukovođenje svakodnevnim poslovima EU. Komesari polažu zakletvu pred Evropskim sudom pravde u Luksemburgu i zaklinju se da će poštovati ugovore i da će potpuno nezavisno izvršavati svoje dužnosti u toku mandata.⁶² Iako postoji po jedan komesar iz svake države članice EU, njihov posao je da brane interese EU kao celine, a ne nacionalne interese.

Izraz Komisija se koristi u užem smislu Kolegijuma komesara (ili Kolegijuma) od 28 članova ili obuhvata i administrativna tela sa oko 23.000 evropskih državnih službenika podeljenih u sektore koji se nazivaju generalni direktorati (DG), koji su odgovorni za različite oblasti politike⁶³ i usluge.⁶⁴ Proceduralni jezici EK su engleski, francuski i nemački. Članovi EK i njihovi „kabineti“ (neposredni timovi) imaju sedišta u zgradi Berlemon u Briselu.

Evropska komisija je podeljena u sektore koji izrađuju politike za konkretne oblasti. Na čelu svakog sektora je komesar. 28 komesara (Kolegijum) donosi odluke o političkim i strateškim pravcima EK, a takođe predlažu zakone, programe finansiranja i godišnji budžet koje Parlament i Savet treba da razmotre i usvoje. Uopšteno, EK radi pod vođstvom predsednika. Novi kolegijum komesara imenuje se svakih 5 godina.

⁶² Evropska komisija polaže zakletvu da će poštovati ugovore EU, saopštenje za štampu, dostupno na: http://europa.eu/rapid/press-release_IP-10-487_en.htm (pristupljeno 2. 3. 2017).

⁶³ Generalni direktorati izrađuju, sprovode i upravljaju politikom, zakonima i programima finansiranja EU.

⁶⁴ Pravilnik Komisije, 1. 1. 2001, Sl. list br. L 308 od 8. 12. 2000.

Odgovornost

Demokratski nadzor nad radom Evropske komisije vrši Evropski parlament, koji ima pravo da odobri ili raspusti čitavo političko vođstvo Komisije. Evropska komisija je takođe odgovorna za realizaciju budžeta EU u praksi. Svake godine Parlament bira da li će podržati (ili neće) način na koji EK upravlja budžetom EU. Ovaj proces se naziva izvršenje. Parlament svoje odluke zasniva na nekoliko izveštaja Evropskog suda revizora i Evropske komisije, uključujući i godišnji izveštaj o upravljanju i učinku za budžet EU.⁶⁵

Službenik za zaštitu podataka

U EK, Službenik za zaštitu podataka (DPO) nezavisno obezbeđuje da Evropska komisija tačno primenjuje odredbe Uredbe 45/2001, kojom se štite podaci o ličnosti pojedinaca. Službenik za zaštitu podataka vodi javni registar u kojem su objašnjene sve radnje koje obavlja EK i koje obuhvataju obradu podataka o ličnosti. Svaka institucija ima jednog ili više službenika za zaštitu podataka da bi se obezbedila primena principa zaštite podataka o ličnosti u instituciji.

Komisija je imenovala Koordinatora za zaštitu podataka (DPC) u svakom generalnom direktoratu. To je opravdano veličinom institucije i potrebom za postojanjem rada u smenama u različitim generalnim direktoratom. Takođe postoji poseban službenik za zaštitu podataka za Evropsku kancelariju za sprečavanje prevara (OLAF).⁶⁶

Schrems v Facebook

Dva najvažnija međunarodna slučaja u vezi sa privatnošću u skorijoj istoriji nastala su iz žalbi protiv Fejsbuka koje je irskom Povereniku

⁶⁵ https://ec.europa.eu/info/about-european-union/organisational-structure/political-leadership_en (pristupljeno 2. 3. 2017).

⁶⁶ Ibid.

za zaštitu podataka podneo austrijski zagovornik zaštite privatnosti Maks Šrems. Šrems je u žalbama doveo u pitanje prenos njegovih podataka (i podataka građana EU uopšteno) Sjedinjenim Američkim Državama od strane Fejsbuka, koji je osnovan u Irskoj. Prvi Šremsov slučaj ("Schrems I") vodio je Sud pravde Evropske unije 6. oktobra 2015. godine da bi se poništio sporazum "Safe Harbour" (Sigurna luka), kojim je bio uređen prenos podataka između EU i SAD. Nakon što je taj slučaj iznesen pred organom za zaštitu podataka Irske, Poverenik je podneo drugu tužbu ("Schrems II") pred Visokim sudom Irske da bi se utvrdilo da li „standardne ugovorne klauzule“ koje je Fejsbuk koristio za odobravanje prenosa podataka u SAD nakon poništavanja sporazuma pružaju adekvatnu zaštitu za građane EU.⁶⁷

Zakonodavstvo o prenosima podataka: Direktiva o zaštiti podataka, Safe Harbour i Privacy Shield

Slučajevi Šrems se bave jednom od osnovnih tenzija između zakonodavstava o privatnosti EU i SAD i međunarodnim sporazumima i ugovorima koji su korišćeni za premošćavanje jaza u zaštiti podataka. Ključno pitanje u oba slučaja je da li pravo SAD obezbeđuje adekvatnu zaštitu za podatke o ličnosti koja je potrebna da bi se dozvolili međunarodni prenosi podataka prema pravu EU.

Za razliku od Sjedinjenih Američkih Država, podrazumevano pravilo u EU je da su prenosi podataka zabranjeni; prenos podataka o ličnosti dozvoljen je samo ako su ispunjeni određeni kriterijumi. Evropska direktiva za zaštitu podataka je zakonodavni akt EU koji otežljuje ovu normu. U Direktivi se navodi da prenos podataka o ličnosti u treću zemlju može da se vrši samo ako ta zemlja obezbeđuje adekvatan nivo zaštite podataka. Direktiva takođe propisuje da EK može da utvrdi da treća zemlja obezbeđuje adekvatan nivo zaštite. Ako EK usvoji odluku kojom se to potvrđuje, može se vršiti prenos podataka o ličnosti u tu treću zemlju.

⁶⁷ <https://epic.org/privacy/intl/schrems/> (pristupljeno 13. 3. 2017).

EK je u julu 2000. godine usvojila odluku kojom se proglašava da Sjedinjene Američke Države obezbeđuju adekvatne mere za zaštitu podataka. Odluka Komisije je bila zasnovana na okviru Safe Harbour. Sporazum Safe Harbour se sastojao od principa zaštite podataka kojim su američka privredna društva mogla dobrovoljno da se prijave za vršenje prekograničnih prenosa podataka. Dakle, zaštita za podatke korisnika oslanjala se na samoprocenu i samosertifikaciju od strane privatnih privrednih društava.⁶⁸

Kako je detaljno opisano u daljem tekstu, Sud pravde Evropske unije je u oktobru 2015. godine presudio da je okvir Safe Harbour nevažeći.

Ubrzo nakon toga EU i SAD su počele da pregovaraju o sporazumu koji će ga zameniti: Privacy Shield (Štit privatnosti) između EU i SAD. EK je usvojila Privacy Shield u julu 2016. godine i privredna društva iz SAD su započela samosertifikaciju i prenos podataka prema ovom sporazumu. Međutim, Privacy Shield ima dosta sličnih ili istih problema kao i okvir Safe Harbour, uključujući i oslanjanje na samosertifikaciju od strane privrednih društava iz SAD.

Schrems I (Safe Harbour): Max Schrems v. Irish Data Protection Commissioner

Ovaj slučaj je nastao iz postupka pred irskim Poverenikom za zaštitu podataka (DPC) koji je pokrenuo Maks Šrems, student doktorskih studija i aktivista za zaštitu privatnosti iz Austrije.

Podaci koje je Šrems, korisnik Fejsbuka, davao Fejsbuku prenošeni su iz zavisnog privrednog društva Fejsbuka u Irskoj (Facebook Ireland) na servere Fejsbuka u Sjedinjenim Američkim Državama (Facebook, Inc.). Šrems je podneo žalbu irskom organu za zaštitu podataka, zauzimajući stav da, u svetlu onoga što je Edvard Snouden

⁶⁸ <https://epic.org/privacy/intl/schrems/> (pristupljeno 13. 3. 2017).

2013. godine otkrio u vezi sa aktivnostima obaveštajnih službi Sjedinjenih Američkih Država (posebno Nacionalne agencije za bezbednost), pravo i praksa SAD ne nude stvarnu zaštitu od nadzora nad podacima prenesenim u SAD od strane te zemlje. Irski organ je odbio žalbu zato što je Komisija, prema odluci od 26. jula 2000. godine, smatrala da SAD u okviru sporazuma "Safe Harbour" obezbeđuju adekvatan nivo zaštite prenešenih podataka o ličnosti.⁶⁹

Šrems je podneo žalbu na odluku Poverenika za zaštitu podataka pred Visokim sudom Irske. Sud je odlučio da obustavi postupak i uputi sledeće pitanje SPEU za preliminarnu presudu:

Može li i/ili mora li nacionalni nadzorni organ za zaštitu podataka da vrši sopstveno ispitivanje adekvatnosti zaštite podataka u trećoj zemlji ili je Poverenik u potpunosti obavezan odlukom Komisije?

Generalni advokat Iv Bot je 23. septembra 2015. godine objavio mišljenje o ovom slučaju. U mišljenju Generalnog advokata se navodi da sporazum Safe Harbour, koji je dozvoljavao prenos podataka o ličnosti iz EU u SAD, mora da bude raskinut zato što aranžman nije obezbedio neophodnu pravnu zaštitu prema pravu EU i zbog toga „mora da bude proglašen nevažećim“. SPEU je objavio presudu u oktobru 2015. godine, u kojoj se složio sa Generalnim advokatom i poništio sporazum Safe Harbour. Sud je presudio da (1) nacionalni organi za zaštitu podataka imaju pravo da ispituju adekvatnost prenosa podataka u okviru sporazuma Safe Harbour između EU i SAD ili bilo kojeg drugog sporazuma zaključenog u skladu sa odlukom Evropske komisije o adekvatnosti za to pitanje, i (2) sporazum Safe Harbour treba da bude nevažeći zbog nedostatka adekvatnosti.⁷⁰

⁶⁹ <https://epic.org/privacy/intl/schrems/> (pristupljeno 13. 3. 2017).

⁷⁰ Ibid.

Nakon presude SPEU, Šrems je podneo ažuriranu žalbu irskom Povereniku za zaštitu podataka zasnovanu na korišćenju „standardnih ugovornih klauzula“ od strane Fejsbuka za odobravanje prenosa podataka između EU i SAD, što je obezbedilo osnovu za novi slučaj pred Visokim sudom Irske. Ubrzo nakon odluke SPEU, Visoki sud Irske poništio je prethodnu odluku irskog Poverenika za zaštitu podataka da ne ispituje firmu Facebook Ireland u vezi sa optužbama iz prve Šremsove žalbe. Irski Poverenik za zaštitu podataka je zatim započeo istragu. Razmatrao je dva ključna pitanja: da li SAD obezbeđuju adekvatan nivo zaštite za korisnike iz EU čiji se podaci prenose i, ako ne obezbeđuje, da li standardne ugovorne klauzule (SCC) koje koriste firme Facebook Ireland i Facebook, Inc. za regulisanje prenosa tih podataka mogu da podignu nivo zaštite, a da prenos podataka ipak bude dozvoljen? Istovremeno, Šrems je ažurirao žalbu protiv Fejsbuka podnetu Povereniku za zaštitu podataka i tvrdio da zakonodavstvo SAD o nadzoru nije u skladu sa zahtevima propisanim pravom EU, uključujući i presudu SPEU u odluci o sporazumu Safe Harbour. SPEU je zaključio da SAD moraju da izmene „domaće zakone“ i „međunarodne obaveze“ kako bi obezbedile suštinski istu zaštitu privatnosti i podataka kao Evropska unija. Pored toga, Šrems je tvrdio da standardne ugovorne klauzule ne obezbeđuju adekvatan nivo zaštite neophodan da bi se na drugi način odobrili prenosi podataka.⁷¹

Irski Poverenik za zaštitu podataka je u maju 2016. godine objavio nacrt Odluke u kojoj je saopštio svoj preliminarni stav: da pravo SAD ne obezbeđuje na adekvatan način pravne lekove građanima EU i da standardne ugovorne klauzule ne mogu da reše problem nedostataka prava SAD. Zbog toga je irski Poverenik za zaštitu podataka predložio da predmetne ugovorne klauzule budu nevažeće prema pravu EU. Međutim, irski Poverenik za zaštitu podataka je

⁷¹ <https://epic.org/privacy/intl/schrems/> (pristupljeno 13. 3. 2017).

zaključio da kao predstavnik jedne nacije u EU sa ograničenim ovlašćenjem nije u mogućnosti da proglasi klauzule nevažećima prema pravu EU; irski Poverenik za zaštitu podataka je tvrdio da je Evropska komisija smatrala da standardne ugovorne klauzule objavljene na osnovu širih ovlašćenja Evropske komisije odobravaju prenos podataka. Irski Poverenik za zaštitu podataka izneo je stav da bez utvrđivanja da su klauzule zaista nevažeće ne mogu da završe istragu Fejsbuka.⁷²

Zbog toga je irski Poverenik za zaštitu podataka ponovo izneo slučaj pred Visokim sudom Irske i tražio upućivanje pred SPEU pitanja da li su odluke o standardnim ugovornim klauzulama važeće prema Povelji o osnovnim pravima.

Saslušanje u okviru ovog postupka započeto je u utorak 7. februara 2017. godine u Visokom sudu (Privredno odeljenje) pred sudijom Karolinom Kostelo. Uvodne predstavke podneo je Poverenik za zaštitu podataka, a uvodne napomene dali su i Fejsbuk i Šrems.

Poverenik za zaštitu podataka je ukratko naveo sledeće: nekoliko statuta, odredaba i presuda. Uputio je na Članove 7, 8, 47, 52. i 53. Povelje o osnovnim pravima i Član 16. Ugovora o funkcionisanju Evropske unije pre nego što je prešao na Članove 25. i 26. Direktive 95/46/EZ. Uputio je na odluku Evropske komisije o sporazumu Safe Harbour (br. 2000/520) i na nekoliko odluka SPEU u vezi sa zaštitom podataka, uključujući i slučajeve *Digital Rights v. Communications Minister*, *Schrems v. Data Protection Commissioner* i *Digital Rights Ireland*.

Pored toga, Poverenik za zaštitu podataka naveo je nekoliko zakona SAD, uključujući i delove Zakona o nadzoru nad stranim obaveštajnim službama, 50 U.S.C. §§ 1801 et seq., i slučaj koji je od značaja za ove odredbe, *Al Haramain Islamic Foundation v. Obama*, 705 F.3d 845 (9th Cir. 2012), u kojem je Apelacioni sud za devetu oblast izneo stav

⁷² <https://epic.org/privacy/intl/schrems/> (pristupljeno 13. 3. 2017).

da Sjedinjene Američke Države ne mogu da se smatraju odgovornima prema Članu § 1810 Zakona o nadzoru nad stranim obaveštajnim službama budući da ova odredba ne uključuje eksplicitno odricanje od suverenog imuniteta. Poverenik za zaštitu podataka je takođe uputio na Zakon o privatnosti elektronskih komunikacija (ECPA), Zakon o prisluškivanju i Zakon o uskladištenim komunikacijama, Zakon o privatnosti i Zakon o sudskoj zaštiti. Takođe, Poverenik za zaštitu podataka predstavio je i skorašnju odluku Okružnog suda u slučaju *Fikre v. FBI*, 142 F. Supp. 3d 1152 (D. Ore. 2015), u kojoj je iznet stav da i nameravano i slučajno kršenje zakonskih odredaba može da predstavlja „namerno“ kršenje prema Članu § 2712. Ovaj odeljak predstavlja odricanje od suverenog imuniteta ako vlast namerno prekrši bilo koju odredbu Zakona o prisluškivanju, Zakona o uskladištenim komunikacijama ili tri nabrojane odredbe Zakona o nadzoru nad stranim obaveštajnim službama: § 1806(a), § 1825(a) ili § 1845(a). Poverenik za zaštitu podataka je takođe naveo pravna sredstva dostupna prema Zakonu o privatnosti i predstavio dve odluke Vrhovnog suda kojima se ta pravna sredstva ograničavaju: slučaj *FAA v. Cooper*, 132 S. Ct. 1441 (2012), u kojem je sud presudio da se zakon nije odrekao suverenog imuniteta u odnosu na tužbe protiv Vlade radi nadoknađivanja nematerijalne štete, i slučaj *Doe v. Chao*, 540 U.S. 614 (2004), gde je presuđeno da tužioci ne mogu da nadoknade minimalnu propisanu štetu prema Zakonu o privatnosti ukoliko ne mogu da dokažu „stvarnu štetu“.⁷³

Još uvek nije doneta odluka o ovom slučaju.

⁷³ <https://epic.org/privacy/intl/schrems/> (pristupljeno 2. 3. 2017).

2.2. RADNA GRUPA ZA ZAŠTITU PODATAKA ČLAN 29

Radna grupa Član 29, koju čine predstavnici svih organa za zaštitu podataka EU koje je imenovala svaka država članica EU, Evropski supervizor za zaštitu podataka (EDPS) (organ osnovan za institucije i tela EU) i Evropska komisija, osnovana je u skladu sa Članom 29. Direktive 95/46/EZ. Ima nadzorni status i postupa nezavisno.⁷⁴

Radna grupa (RG29) bira predsedavajućeg i zamenike predsedavajućeg. Njihov mandat traje dve godine. Oni mogu da budu ponovo imenovani na te položaje. Sekretarijat Radne grupe obezbeđuje Komisija.

RG29 je osnovana radi ostvarivanja nekoliko primarnih ciljeva:

- davanje stručnih mišljenja na nivou država članica Evropskoj komisiji o pitanjima u vezi sa zaštitom podataka;
- promovisanje jedinstvene primene opštih principa direktiva u svim državama članicama kroz saradnju između nadzornih organa za zaštitu podataka;
- davanje saveta EK o svim merama EU koje utiču na prava i slobode fizičkih lica u vezi sa obradom podataka o ličnosti i privatnošću;
- davanje preporuka široj javnosti i institucijama EU o pitanjima u vezi sa zaštitom lica u odnosu na obradu podataka o ličnosti i privatnost u EU.⁷⁵

RG29 je usvojila svoj Poslovnik⁷⁶, Smernice i najčešće postavljana pitanja o pravu na prenosivost podataka: Smernice o pravu na prenosivost podataka⁷⁷ i WP242 PRILOG – Najčešće postavljana

⁷⁴ http://ec.europa.eu/justice/data-protection/index_en.htm (pristupljeno 2. 3. 2017).

⁷⁵ http://ec.europa.eu/justice/data-protection/article-29/files/tasks-art-29_en.pdf (pristupljeno 2. 3. 2017).

⁷⁶ Poslovnik, Brisel, 15. februar 2010, dostupno na: http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf (pristupljeno 2. 3. 2017).

⁷⁷ Smernice o pravu na prenosivost podataka, 13. decembar 2016, dostupno na: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf (pristupljeno 2. 3. 2017).

pitanja⁷⁸; Smernice i najčešće postavljana pitanja o službenicima za zaštitu podataka (DPO): Smernice o službenicima za zaštitu podataka ("DPOs")⁷⁹ i WP243 PRILOG – Najčešće postavljana pitanja⁸⁰; Smernice i najčešće postavljana pitanja o vodećem nadzornom organu: Smernice za vodećeg nadzornog organa rukovaoca podataka ili obrađivača⁸¹ i WP244 PRILOG II – Najčešće postavljana pitanja⁸².

Pravni okvir

Pravna osnova za Radnu grupu su Članovi 29. i 30. Direktive 95/46/EZ Evropskog parlamenta i Saveta, od 24. oktobra 1995, o zaštiti pojedinaca prilikom obrade podataka o ličnosti i o slobodnom kretanju tih podataka⁸³ i Član 15. Direktive 2002/58/EZ Evropskog parlamenta i Saveta, od 12. jula 2002, o obradi podataka o ličnosti i zaštiti privatnosti u sektoru elektronskih komunikacija (Direktiva o privatnosti i elektronskim komunikacijama)⁸⁴.

⁷⁸ WP242 PRILOG – Najčešće postavljana pitanja, dostupno na: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf (pristupljeno 6. 3. 2017).

⁷⁹ Smernice o službenicima za zaštitu podataka ("DPO"), 13. decembar 2016, dostupno na: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf (pristupljeno 6. 3. 2017).

⁸⁰ WP243 PRILOG – Najčešće postavljana pitanja, dostupno na: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf (pristupljeno 6. 3. 2017).

⁸¹ Smernice za određivanje vodećeg nadzornog organa rukovaoca podataka ili obrađivača, 13. decembar 2016, dostupno na: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf (pristupljeno 6. 3. 2017).

⁸² WP244 PRILOG II – Najčešće postavljana pitanja, dostupno na: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_annexii_en_40858.pdf (pristupljeno 6. 3. 2017).

⁸³ Direktiva 95/46/EZ.

⁸⁴ Direktiva 2002/58/EZ.

Mišljenja

RG29 daje mišljenja, preporuke i smernice o primeni nacionalnih mera usvojenih u skladu sa Direktivom 95/46/EZ i Direktivom 2002/58/EZ.

Treba pomenuti dva mišljenja koja se bave konkretnim pitanjima. Prvo je Mišljenje 8/2014 o skorašnjim kretanjima u vezi s internetom stvari (usvojeno 16. septembra 2014)⁸⁵, a drugo je Mišljenje 06/2013 o ponovnom korišćenju otvorenih podataka i informacija iz javnog sektora ("IJS") (usvojeno 5. juna 2013).⁸⁶ Radna grupa je takođe dala mišljenje o računarstvu u oblaku, dronovima, „kolačićima“, aplikacijama i pametnim uređajima i podacima o geolokaciji.

RG29 je dala tri mišljenja o konceptima ZPL. Mišljenje 05/2014 o tehnikama anonimizacije (usvojeno 10. aprila 2014)⁸⁷, Mišljenje 03/2013 o ograničavanju svrhe (usvojeno 2. aprila 2013)⁸⁸ i Mišljenje 15/2011 o definiciji pristanka (usvojeno 13. jula 2011).⁸⁹

RG29 je takođe dala mišljenja o presudama ESP, na primer Smernice o sprovođenju presude Suda pravde Evropske unije u slučaju "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/121 (usvojene 26. novembra 2014)⁹⁰ i Ažurirani dodatak Mišljenju 8/2010 o važećem pravu na osnovu kojeg se razmatra presuda SPEU u slučaju Google

⁸⁵ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 6. 3. 2017).

⁸⁶ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf (pristupljeno 6. 3. 2017).

⁸⁷ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (pristupljeno 6. 3. 2017).

⁸⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (pristupljeno 6. 3. 2017).

⁸⁹ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (pristupljeno 6. 3. 2017).

⁹⁰ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (pristupljeno 6. 3. 2017).

Spain (usvojen 16. decembra 2015)⁹¹ ili o slučaju Šrems i poništavanju Direktive o zadržavanju podataka.

Mišljenje 8/2014 o najnovijim kretanjima u oblasti interneta stvari

Mišljenje se odnosi na infrastrukturu u kojoj su na milijarde senzora ugrađenih u svakodnevne uređaje – „stvari“ kao takve ili stvari koje su povezane sa drugim predmetima ili licima – projektovani da snimaju, obrađuju i čuvaju podatke a, s obzirom na to da su povezani s jedinstvenim identifikatorima, takođe i da uzajamno deluju sa drugim uređajima i sistemima koristeći mrežne kapacitete. Odnosi se na korisnike podatke specifične za konkretno okruženje i posebno prati i analizira navike korisnika.⁹²

Internet stvari (engl. *Internet of Things* – IoT) je na pragu da postane sastavni deo života evropskih građana. Održivost mnogih projekata interneta stvari tek treba da bude potvrđena, ali već su dostupne „pametne stvari“ koje prate i komuniciraju s našim domovima, automobilima, radnim okruženjem i fizičkim aktivnostima. Povezani uređaji već danas uspešno zadovoljavaju potrebe građana EU na masovnim tržištima samokvantifikacije i domotike. Internet stvari, dakle, ima značajnu perspektivu rasta za veliki broj inovativnih i kreativnih privrednih društava u EU, bilo da su velika ili mala, koja posluju na tim tržištima.

Pa ipak, ove očekivane prednosti treba sagledati i u svetlu brojnih izazova za privatnost i bezbednost koji se povezuju s internetom stvari. Postavljaju se mnoga pitanja vezana za ugroženost tih uređaja, koji se često koriste izvan tradicionalne strukture informacionih tehnologija i nemaju ugrađen dovoljan stepen bezbednosti. Gubitak podataka, inficiranje štetnim softverom (engl. *malware*), ali

⁹¹ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf (pristupljeno 6. 3. 2017).

⁹² http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 7. 3. 2017).

i neovlašćen pristup podacima o ličnosti, korišćenje nosivih uređaja na način koji zadire u privatnost ili nezakonit nadzor su rizici na koje akteri interneta stvari moraju da odgovore da bi privukli potencijalne krajnje korisnike svojih proizvoda ili usluga.

Ako ostavimo po strani zakonitost i tehničku usaglašenost, ovde se radi o posledicama koje sve to može imati za društvo u celini. Organizacije koje privatnost i zaštitu podataka smatraju jednim od najvažnijih aspekata razvoja proizvoda biće u mogućnosti da obezbede da njihovi proizvodi i usluge budu u skladu s načelima ugrađene privatnosti i da budu opremljeni podešavanjima koja doprinose zaštiti privatnosti kakvu građani EU očekuju.

Nosivo računarstvo

Pod nosivim računarstvom (engl. *wearable computing*) podrazumevaju se svakodnevni predmeti i odeća, kao što su ručni satovi i naočare, u koje su ugrađeni senzori da bi se proširila njihova funkcionalnost. Nosive stvari će verovatno brzo biti prihvaćene, jer povećavaju upotrebnu vrednost svakodневnih predmeta koji su korisniku poznati; štaviše, jedva da se i razlikuju od sličnih predmeta koji nisu povezani na mrežu. U njih mogu da budu ugrađene kamere, mikrofoni i senzori koji mogu da snimaju i prenose podatke proizvođaču uređaja. Osim toga, dostupnost aplikacionog programskog interfejsa (API) za nosive uređaje (npr. Android Wear⁹³) takođe podržava i izradu aplikacija od strane trećih lica, koja tako mogu dobiti pristup podacima koje ti predmeti prikupljaju.⁹⁴

Samokvantifikacija

Predmeti za samokvantifikaciju (engl. *quantified self*) projektovani su da ih redovno nose osobe koje žele da beleže informacije o sopstvenim navikama i životnom stilu. Primera radi, neko možda želi

⁹³ <http://developer.android.com/wear/index.html> (pristupljeno 6. 3. 2017).

⁹⁴ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 7. 3. 2017).

da nosi uređaj za praćenje spavanja da bi dobio detaljne podatke o obrascima spavanja. Drugi uređaji prate pokrete, npr. brojači aktivnosti koji neprekidno mere i izveštavaju o kvantitativnim indikatorima vezanim za fizičke aktivnosti pojedinca, npr. broj utrošenih kalorija ili prepešaćenu udaljenost.

Neki predmeti, pak, mere telesnu težinu, puls i pokazatelje zdravstvenog stanja. Posmatranjem trendova i promena u ponašanju tokom vremena moguće je analizirati prikupljene podatke da bi se izveli određeni kvalitativni podaci o zdravstvenom stanju, uključujući i procenu kvaliteta i efekata fizičke aktivnosti na osnovu unapred utvrđenih graničnih vrednosti i mogućeg prisustva simptoma bolesti.⁹⁵

Nošenje senzora za samokvantifikaciju je često neophodno u određenim uslovima da bi se dobile relevantne informacije. Primera radi, akcelerometar postavljen na pojas lica na koje se podaci odnose, uz odgovarajuće algoritme, može da meri pokrete abdomena (sirovi podaci), da izvede informacije o ritmu disanja (agregirani podaci i izvedene informacije) i da prikaže nivo stresa lica na koje se podaci odnose (podaci za prikaz). Na nekim uređajima se korisniku prikazuju samo ovi poslednji podaci, ali proizvođač uređaja ili pružalac usluge može da ima pristup mnogo većoj količini podataka koji se mogu naknadno analizirati.

Samokvantifikacija predstavlja izazov u pogledu prikupljenih podataka koji se odnose na zdravstveno stanje, te su stoga potencijalno osetljivi, kao i u pogledu obimnog prikupljanja tih podataka. Zapravo, pošto je ovaj pokret fokusiran na motivisanje korisnika da ostanu zdravi, postoje mnoge veze s ekosistemom e-zdravlja. Međutim, u novijim ispitivanjima osporena je tačnost merenja i zaključaka koji se iz njih izvode.⁹⁶

⁹⁵ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 7. 3. 2017).

⁹⁶ <http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results> (pristupljeno 6. 3. 2017).

Domotika – automatizacija doma

Danas uređaji interneta stvari mogu da budu postavljeni i u kancelarije ili domove, npr. „povezane“ sijalice, termostati, detektori dima, meteorološke stanice, mašine za pranje rublja ili štednjake moguće je kontrolisati daljinski putem interneta. Primera radi, stvari koje sadrže senzore pokreta mogu da detektuju i beleže kada je korisnik kod kuće i kakvi su mu obrasci kretanja i da eventualno aktiviraju unapred zadate radnje (npr. uključivanje svetla ili promena temperature u prostoriji). Većina uređaja za automatizaciju doma je stalno povezana na mrežu i može da šalje podatke proizvođaču.⁹⁷

Jasno je da domotika donosi sa sobom specifične izazove vezane za zaštitu podataka i privatnost, budući da analiza obrazaca korišćenja u takvom kontekstu može da otkrije podatke o životnom stilu stanara, njihovim navikama ili izborima, ili jednostavno o tome da li su kod kuće.

Tri navedene kategorije uređaja su reprezentativne za glavne probleme sa stanovišta privatnosti vezane za internet stvari u stanju u kojem se sada nalazi. Treba, međutim, istaći da ove kategorije nisu međusobno isključive: na primer, „nosivi“ uređaj, kao što je pametni sat, može da se koristi za praćenje broja otkucaja srca, tj. za samokvantifikaciju.

Nedostatak kontrole i informaciona asimetrija

Zbog potrebe da se sveprisutne usluge pružaju na nenametljiv način, korisnici u praksi mogu da se nađu pod nadzorom trećih lica. To može da dovede do situacija u kojima korisnik gubi svaku kontrolu nad prenošenjem svojih podataka, u zavisnosti od toga da li se prikupljanje i obrada tih podataka vrši na transparentan način ili ne.

⁹⁷ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 8. 3. 2017).

Valjanost pristanka korisnika

Korisnik u mnogim slučajevima ne mora ni da bude svestan obrade podataka koju vrše određeni predmeti. Taj nedostatak informacija predstavlja značajnu prepreku za dokazivanje postojanja valjanog pristanka u skladu sa zakonom EU, jer lice na koje se podaci odnose mora da bude informisano. U takvim okolnostima ne može se osloniti na pristanak kao pravni osnov za obradu podataka u skladu sa zakonom EU.⁹⁸

Takođe, nosivi uređaji, kao što su pametni satovi, nisu uočljivi⁹⁹: većina posmatrača ne zna razliku između običnog sata i sata povezanog na mrežu, a ovaj drugi može u sebi da sadrži kamere, mikrofone i senzore pokreta koji mogu da snimaju i prenose podatke bez znanja, a kamoli saglasnosti, pojedinca. To povlači za sobom pitanje prepoznavanja obrade podataka putem nosivih računarskih uređaja, što može da se reši predviđanjem odgovarajućih oznaka koje bi bile stvarno vidljive licima na koja se podaci odnose.

Pored toga, klasični mehanizmi za pribavljanje pristanka lica mogu biti teško primenjivi u slučaju interneta stvari, što dovodi do „nekvalitetnog“ pristanka zasnovanog na nedostatku informacija ili do faktičke nemogućnosti davanja preciznog pristanka u skladu sa izraženim željama lica.

Zaključci izvedeni iz podataka i promena svrhe obrade

Usled povećanja količine podataka koje generiše internet stvari, u kombinaciji s modernim tehnikama vezanim za analizu i unakrsno povezivanje podataka, može doći do korišćenja podataka u sekundarne svrhe, bilo da su one povezane sa svrhom za koju su podaci

⁹⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 8. 3. 2017).

⁹⁹ Kao što je opisano u Mišljenju 02/2013 o aplikacijama na pametnim uređajima, kod nosivih računarskih uređaja takođe se uočavaju i izazovi koji proističu iz stalnog prikupljanja podataka od drugih lica u neposrednoj blizini tokom dužeg perioda.

prvobitno obrađeni ili ne. Na primer, treća lica koja zahtevaju pristup podacima koje prikupljaju druga lica možda će hteti da te podatke upotrebe u sasvim druge svrhe.

Nametljivo isticanje obrazaca ponašanja i profilisanje

Iako različiti predmeti odvojeno prikupljaju izolovane informacije, na osnovu dovoljne količine prikupljenih i dodatno analiziranih podataka moguće je otkriti specifične aspekte navika, ponašanja i sklonosti pojedinca. Kao što je gore objašnjeno, formiranje znanja na osnovu trivijalnih ili čak anonimnih podataka biće olakšano zahvaljujući masovnom prisustvu senzora, što će usloviti razvoj značajnih mogućnosti profilisanja. Osim toga, analitika zasnovana na informacijama zabeleženim u okruženju interneta stvari može da omogući otkrivanje još detaljnijih obrazaca u životu i ponašanju pojedinca.

U stvari, ovaj trend će verovatno uticati na stvarno ponašanje pojedinca, baš kao što je dokazano da je intenzivno korišćenje video nadzora uticalo na ponašanje građana na javnim mestima. Sa internetom stvari, potencijalni nadzor sada može da zadre i u najintimniju sferu života pojedinca, uključujući i dom. To će stvoriti pritisak na pojedinca da izbegava neuobičajeno ponašanje kako bi sprečio otkrivanje nečega što bi moglo da se protumači kao anomalija. Takav trend bi predstavljao ozbiljno zadiranje u privatni život i intimu pojedinaca i trebalo bi ga vrlo pažljivo pratiti.¹⁰⁰

Ograničena mogućnost zadržavanja anonimnosti prilikom korišćenja usluga

Potpun razvoj mogućnosti interneta stvari može da smanji postojeće mogućnosti anonimnog korišćenja usluga i da uopšteno ograniči mogućnost da se ostane neprimećen.

¹⁰⁰ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 9. 3. 2017).

Bezbednosni rizici: bezbednost naspram efikasnosti

Internet stvari donosi sa sobom nekoliko bezbednosnih izazova, usled činjenice da zahtevi bezbednosti i ograničenja resursa primoravaju proizvođače uređaja da balansiraju između efikasnosti baterije i bezbednosti uređaja. Konkretno, još uvek nije jasno na koji način će proizvođači uređaja uspostaviti ravnotežu između sprovođenja mera poverljivosti, integriteta i dostupnosti na svim nivoima redosleda obrade i potrebe za optimalnim iskorišćenjem računarskih resursa – i energije – po predmetima i senzorima.¹⁰¹

Primenljivost prava EU

Relevantni zakonski okvir za pitanja privatnosti i zaštite podataka koja postavlja internet stvari u EU čini Direktiva 95/46/EZ, kao i posebne odredbe Direktive 2002/58/EZ izmenjene i dopunjene Direktivom 2009/136/EZ¹⁰².

Ovaj okvir se primenjuje kada su ispunjeni uslovi za primenu iz Člana 4. Direktive 95/46/EZ. Radna grupa je pružila detaljna uputstva u vezi s tumačenjem odredaba Člana 4, i to u svom Mišljenju 8/2010¹⁰³ o pravu koje se primenjuje. U skladu sa Članom 4-1(a) Direktive, nacionalni zakon države članice se primenjuje na svu obradu podataka o ličnosti koja se vrši „u okviru delatnosti poslovne jedinice“ rukovoca na teritoriji te države članice. Ovaj pojam poslovne jedinice u kontekstu ekonomije bazirane na internetu Evropski sud pravde nedavno je protumačio veoma široko¹⁰⁴.

¹⁰¹ <http://www.dataprotection.ro/servlet/ViewDocument?id=1088> (pristupljeno 18. 3. 2017).

¹⁰² Direktiva 2009/136/EZ Evropskog parlamenta i Saveta, od 25. novembra 2009, kojom se menja i dopunjuje Direktiva 2002/22/EZ o univerzalnim uslugama i pravima korisnika u vezi s elektronskim komunikacionim mrežama i uslugama, Direktiva 2002/58/EZ o obradi podataka o ličnosti i zaštiti privatnosti u sektoru elektronskih komunikacija i Uredba (EZ) br. 2006/2004 o saradnji između nacionalnih organa odgovornih za sprovođenje Zakona o zaštiti potrošača, Sl. list br. L 337, 18. 12. 2009, str. 11–36.

¹⁰³ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf (pristupljeno 6. 3. 2017).

¹⁰⁴ SPEU, predmet C-131/12, 13. maj 2014, stavovi 45 do 60.

Nacionalni zakoni države članice se takođe primenjuju i u slučajevima kada rukovalac nema poslovnu jedinicu na teritoriji Zajednice, ali koristi „opremu“ koja se nalazi na teritoriji te države članice (Član 4-1(v)). Prema tome, čak iako akter u internet stvari, koji ispunjava uslove da se smatra rukovaocem podataka u skladu s Direktivom 95/46/EZ, nema poslovnu jedinicu u EU u smislu Člana 4-1(a) (nezavisno od toga da li se bavi razvojem, distribucijom ili funkcionisanjem usluga interneta stvari), na njega će se verovatno primenjivati pravo EU u delu u kojem obrađuje podatke prikupljene pomoću „opreme“ korisnika koja se nalazi u EU.

Akteri interneta stvari kao rukovaoci podataka sa sedištem u EU

Koncept rukovaoca podataka i njegova interakcija s pojmom obrađivača podataka ključni su za primenu Direktive 95/46/EZ, jer uslovljavaju odgovornosti različitih organizacija koje učestvuju u vršenju obrade podataka u skladu s pravilima o zaštiti podataka u EU. Za tumačenje pojmova „rukovalac“ i „obrađivač“ akteri mogu da konsultuju mišljenje Radne grupe „Član 29“ br. 1/2010¹⁰⁵, koje sadrži uputstva za primenu ovih koncepata u složenim sistemima sa većim brojem aktera, gde se u mnogim scenarijima samostalno ili zajednički javljaju rukovaoci i obrađivači, sa različitim stepenima samostalnosti i odgovornosti.¹⁰⁶

Štaviše, implementacija interneta stvari već i sama po sebi podrazumeva zajedničko angažovanje većeg broja aktera – proizvođača uređaja, društvenih platformi, aplikacija trećih lica, davalaca uređaja u zakup ili najam, brokera podataka¹⁰⁷ ili platformi podataka.

¹⁰⁵ Mišljenje 01/2010 o konceptima rukovaoca i obrađivača, usvojeno 16. februara 2010. (WP 169), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (pristupljeno 6. 3. 2017).

¹⁰⁶ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 6. 3. 2017).

¹⁰⁷ Brokri podataka kupuju podatke od privrednih društava da bi formirali liste lica koja pripadaju istoj kategoriji ili grupi. Te kategorije i grupe formiraju brokri podataka, a mogu da odražavaju demografske attribute, prihode ili izražena interesovanja za određenu temu ili proizvod.

Pojedinci kao lica na koja se podaci odnose: pretplatnici, korisnici, nekorisnici

Pretplatnici i uopšteno korisnici interneta stvari ispunjavaju uslove da se smatraju licima na koja se podaci odnose u skladu s pravom EU. Ako se podaci koje prikupljaju i pohranjuju koriste isključivo za njihove lične ili kućne potrebe, na njih se primenjuje takozvano „izuzeće za domaćinstva“ iz Direktive 95/46/EZ¹⁰⁸. Međutim, poslovni model u okviru interneta stvari u praksi podrazumeva da se podaci korisnika sistematski prosleđuju proizvođačima uređaja, razvijaačima aplikacija i drugim trećim licima koja se smatraju rukovaocima podataka. Shodno tome, „izuzeće za domaćinstva“ ima ograničenu primenu u kontekstu interneta stvari.

Obrada podataka u okviru internet stvari takođe može da se tiče i lica koja nisu ni pretplatnici, a ni stvarni korisnici interneta stvari. Primera radi, nosivi uređaji, poput pametnih naočara, verovatno prikupljaju podatke i o drugim licima osim samog vlasnika uređaja. Važno je naglasiti da ovaj faktor ne sprečava primenu prava EU u takvim situacijama. Primena pravila EU o zaštiti podataka nije uslovljena vlasništvom nad uređajem ili terminalom, već obradom samih podataka o ličnosti, nezavisno od toga ko je lice na koje se ti podaci odnose.

Pravni osnov za obradu (Član 7. Direktive 95/46)

Akteri interneta stvari koji se smatraju rukovaocima podataka moraju da ispune jedan od zahteva iz Člana 7. ove Direktive da bi obrada podataka o ličnosti bila zakonita. Ti zahtevi se za neke aktere primenjuju uz Član 5(3), u slučajevima kada predmetna obrada podrazumeva više od pohranjivanja informacija ili pristupanja informacijama pohranjenim na terminalnoj opremi korisnika/pretplatnika.¹⁰⁹

¹⁰⁸ Videti Mišljenje 5/2009 o društvenom umrežavanju, usvojeno 12. juna 2009. (WP 163).

¹⁰⁹ U vezi s formulacijom Člana 5(3) i Člana 7(a), videti Mišljenje 02/2013 o aplikacijama na pametnim uređajima, usvojeno 27. februara 2013. godine (WP202), str. 14 i dalje, i Mišljenje 06/2014 o konceptu legitimnih interesa rukovaoca podataka u skladu sa Članom 7. Direktive 95/46/EZ (WP217), str. 26, 32, 46.

Pristanak (Član 7(a)) je prvi zakonski osnov na koji se treba prvenstveno oslanjati u kontekstu interneta stvari, bilo da su u pitanju proizvođači uređaja, društvene platforme ili platforme za čuvanje podataka, davaoci uređaja u zakup ili treća lica koja razvijaju aplikaciju. Radna grupa je u više navrata takođe dala uputstva u vezi sa istovremenom primenom zahteva iz Člana 7(a) i Člana 5(3) Direktive 2002/58/EZ¹¹⁰. Uslovi koji moraju da budu ispunjeni da bi se takav pristanak smatrao valjanim u skladu s pravom EU takođe su određeni u jednom od prethodnih mišljenja Radne grupe.¹¹¹

Članom 7(b) takođe je propisano da je obrada zakonita ako je neophodna radi izvršenja ugovora u kojem je lice na koje se podaci odnose ugovorna strana. Mogućnost primene ovog zakonskog osnova ograničena je kriterijumom „nužnosti“, koji zahteva postojanje direktne i objektivne veze između same obrade i svrhe izvršenja ugovora koje se očekuju od lica na koje se podaci odnose.

Treće, Član 7(đ) dozvoljava obradu podataka o ličnosti kada je potrebna zbog legitimnih interesa čijem ostvarenju teži rukovalac ili treće lica ili lica kojima se podaci otkrivaju, osim kada nad tim interesima preovlađuju interesi osnovnih prava i sloboda lica na koje se podaci odnose – a posebno njegovo pravo na privatnost u odnosu na obradu podataka o ličnosti – koji zahtevaju zaštitu u skladu sa Članom 1(1) Direktive.¹¹²

U svojoj presudi u predmetu Google Spain¹¹³, Evropski sud pravde dao je suštinska uputstva za tumačenje ove odredbe, uz uputstvo koje je već dato u ranijim objedinjenim predmetima ASNEF i FECEMD (C-468/10 i C-469/10). U kontekstu interneta stvari, obrada podataka o ličnosti pojedinca će verovatno značajno uticati na

¹¹⁰ Mišljenje 02/2013 o aplikacijama na pametnim uređajima, usvojeno 27. februara 2013. (WP202), str. 14 i dalje.

¹¹¹ Mišljenje 15/2011 o definiciji pristanka, usvojeno 3. jula 2011. (WP 187).

¹¹² http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 6. 3. 2017).

¹¹³ SPEU, predmet C-131/12, 13. maj 2014, stavovi 74 ff.

njegova, odnosno njena osnovna prava na privatnost i zaštitu podataka o ličnosti u situacijama gde bez uređaja interneta stvari podaci ne bi mogli da budu međusobno povezani, ili bi to bilo moguće samo uz velike teškoće. Do takvih situacija može doći kada se prikupljeni podaci odnose na zdravstveno stanje, dom ili intimu pojedinca, lokaciju i mnoge druge aspekte njegovog, odnosno njenog privatnog života. U svetlu potencijalne ozbiljnosti takvog zadiranja, takva obrada teško da može da se opravda samo ekonomskim interesom koji akter interneta stvari ima u vezi s obradom. U obzir takođe moraju da se uzmu i drugi interesi čijem ostvarenju teži rukovalac podataka ili treće lica, odnosno lica kojima se podaci otkrivaju.¹¹⁴

Načela koja se odnose na valjanost obrade podataka

Načela otelotvorena u Članu 6. Direktive 95/4/EZ zajedno čine kamen-temeljac zakonodavstva o zaštiti podataka u EU.

Podaci o ličnosti se moraju prikupljati i obrađivati pošteno i zakonito. Načelo pravične obrade konkretno nalaže da podaci o ličnosti nikada ne smeju da se prikupljaju i obrađuju bez znanja lica. Ovaj zahtev dodatno dobija na značaju u vezi s internetom stvari, jer su senzori projektovani tako da rade što je moguće neprimetnije. Ipak, rukovaoci koji podacima rukuju na internetu stvari (a pre svega proizvođači uređaja) moraju da obaveste sva lica u geografskoj ili digitalnoj blizini uređaja povezanih na mrežu da se prikupljaju podaci o njima ili njihovom okruženju. Poštovanje ove odredbe je više od puke zakonske obaveze: pošteno prikupljanje podataka jedno je od najvažnijih očekivanja korisnika u vezi s internetom stvari, a posebno u delu koji se odnosi na nosivo računarstvo.

Načelo ograničavanja svrhe podrazumeva da podaci mogu da se prikupljaju samo u navedene, izričite i legitimne svrhe. Svaka dalja obrada koja nije u skladu s tim prvobitnim svrhama bila bi nezakonita u

¹¹⁴ Mišljenje 06/2014 o konceptu legitimnih interesa rukovaoca podataka u skladu sa Članom 7. Direktive 95/46/EZ, usvojeno 9. aprila 2014. (WP217).

skladu s pravom EU. Cilj ovog načela je da korisnicima omogućiti da znaju kako će se i u koje svrhe njihovi podaci koristiti, te da na osnovu toga odluče da li će rukovaocu poveriti svoje podatke. Te svrhe moraju da budu određene pre početka obrade, što isključuje mogućnost iznenadnih promena glavnih uslova obrade. To znači da akteri interneta stvari moraju dobro da sagledaju opravdanost pre nego što počnu sa prikupljanjem bilo kakvih podataka o ličnosti.¹¹⁵

Takođe, podaci koji se prikupljaju o licu moraju da budu krajnje neophodni za konkretnu svrhu koju je rukovalac podataka unapred odredio (načelo svođenja potrebne količine podataka na najmanju moguću meru, odnosno „minimizacije“). Podaci koji nisu neophodni za tu svrhu ne smeju se prikupljati i pohranjivati „za svaki slučaj“ ili zato što će „možda zatrebati kasnije“. Neki akteri smatraju da načelo „minimizacije“ podataka može da ograniči potencijalne mogućnosti interneta stvari i da stoga predstavlja prepreku za inovacije, vođeni idejom da će potencijalne koristi od obrade podataka biti ostvarene kroz istraživačku analizu koja nastoji na pronalaz korelacije i trendove koji nisu uočljivi na prvi pogled. Radna grupa se ne slaže s tom analizom i insistira da načelo „minimizacije“ podataka ima suštinsku ulogu u očuvanju prava na zaštitu podataka koja lica imaju na osnovu prava EU, te da se kao takvo mora poštovati. Ovo načelo konkretno podrazumeva da bi, u slučajevima kada podaci o ličnosti nisu neophodni za funkcionisanje konkretne usluge na internetu stvari, licu na koje se podaci odnose morala barem biti ponuđena mogućnost anonimnog korišćenja usluge.

Članom 6. takođe je propisano da lični podaci koji su prikupljeni i koji se obrađuju u kontekstu interneta stvari ne smeju da se čuvaju duže nego što je neophodno za svrhe za koje su podaci prikupljeni ili za koje su dalje obrađeni. Ovaj test neophodnosti mora da izvrši svaki akter prilikom pružanja konkretne usluge na internetu stvari, jer različiti akteri mogu da vrše obradu u različite svrhe. Primera radi, podaci

¹¹⁵ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 9. 3. 2017).

o ličnosti koje je korisnik dao prilikom prijavljivanja na određenu uslugu na internetu stvari morali bi da budu obrisani čim korisnik otkaže pretplatu. Isto tako, informacije koje je korisnik obrisao sa svog naloga ne bi smele da se čuvaju. Ako korisnik određeno vreme ne koristi uslugu ili aplikaciju, korisnički profil bi trebalo da postane neaktivan. Po isteku dodatnog perioda, podaci bi morali da budu obrisani. Korisnik bi trebalo da bude obavešten pre preduzimanja ovih koraka putem sredstava komunikacije kojima raspolaže predmetni akter.¹¹⁶

Prava lica na koje se podaci odnose

Akteri interneta stvari moraju da poštuju prava lica na koja se podaci odnose, u skladu s odredbama Članova 12. i 14. Direktive 95/46/EZ, i da preduzmu adekvatne organizacione mere. Ova prava nisu ograničena na pretplatnike usluga interneta stvari ili vlasnike uređaja i tiču se svakog lica čiji se podaci o ličnosti obrađuju.¹¹⁷

Pravo pristupa

Članom 12(a) propisano je da lice na koje se podaci odnose ima pravo da od rukovoca dobije obaveštenje u razumljivom obliku o podacima koji se obrađuju i o svim raspoloživim informacijama o njihovom izvoru.

Mogućnost povlačenja pristanka i protivljenja

Lica na koja se podaci odnose moraju da imaju mogućnost povlačenja prethodno datog pristanka na konkretnu obradu podataka i da se usprotive obradi podataka koji se na njih odnose. Ostvarivanje tog prava mora da bude omogućeno bez ikakvih tehničkih ili organizacionih ograničenja ili prepreka, a sredstva pomoću kojih korisnik može da evidentira povlačenje pristanka moraju da budu dostupna, vidljiva i efikasna.

¹¹⁶ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (pristupljeno 9. 3. 2017).

¹¹⁷ Radna grupa, Mišljenje 8/2014 o skorašnjim kretanjima u vezi s internetom stvari, WP 223.

Povlačenje pristanka trebalo bi da bude fino podešeno i da obuhvata: (1) sve podatke koje konkretna stvar prikuplja (npr. zahtev da meteorološka stanica prestane sa prikupljanjem podataka o vlažnosti, temperaturi i zvukovima); (2) konkretnu vrstu podataka koju prikuplja bilo koja stvar (npr. korisnik bi morao da ima mogućnost da prekine prikupljanje podataka bilo kojim uređajem koji snima zvuk, bilo da je u pitanju uređaj za praćenje spavanja ili meteorološka stanica); (3) konkretnu obradu podataka (npr. korisnik može da zahteva da i njegov pedometar i njegov ručni sat prestanu da mu broje korake).¹¹⁸

Dalje, pošto će nosive „stvari povezane na mrežu“ verovatno zameniti postojeće predmete sa uobičajenim funkcionalnostima, rukovaoci podataka trebalo bi da ponude opciju da se deaktivira „povezana“ funkcija konkretne stvari i da se omogući da ona radi kao izvorni predmet koji nije povezan na mrežu (tj. da se deaktivira funkcionalnost povezivanja na mrežu u pametnom satu ili naočarima). Radna grupa je već navela da bi lica na koja se podaci odnose morala da imaju mogućnost da „uvek povuku (svoj) pristanak, bez potrebe za otkazivanjem pružene usluge“¹¹⁹. Ali sa stupanjem OUZP na snagu, samu radnu grupu će zameniti novi Evropski odbor za zaštitu podataka.¹²⁰

¹¹⁸ Radna grupa, Mišljenje 8/2014 o skorašnjim kretanjima u vezi s internetom stvari, WP 223.

¹¹⁹ Mišljenje 13/2011 o geolokacijskim uslugama na mobilnim uređajima, usvojeno 16. maja 2011. (WP185), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf (pristupljeno 6. 3. 2017).

¹²⁰ Član 94. OUZP (Stavljanje van snage Direktive 95/46/EZ):

1. Direktiva 95/46/EZ prestaje da važi 25. maja 2018.

2. Upućivanja na direktivu koja je prestala da važi tumače se kao upućivanja na ovu Uredbu. Upućivanja na Radnu grupu za zaštitu lica u odnosu na obradu podataka o ličnosti, koja je ustanovljena Članom 29. Direktive 95/46/EZ, tumače se kao upućivanja na Evropski odbor za zaštitu podataka ustanovljen ovom Uredbom.

2.3. EVROPSKI NADZORNIK ZA ZAŠTITU PODATAKA

Evropski nadzornik za zaštitu podataka (ENZP) je nezavisno nadzorno telo Evropske unije. Ovo telo osnovano je Uredbom (EZ) br. 45/2001 Evropskog parlamenta i Saveta, od 18. decembra 2001. godine, o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti od strane institucija i tela Zajednice i o slobodnom kretanju takvih podataka. Nezavisno nadzorno telo uspostavljeno ovom Uredbom nadzire primenu odredaba ove Uredbe na sve operacije obrade koje sprovode institucije ili tela Zajednice (Član 1. stav 2). Dakle, ENZP nadgleda obradu podataka o ličnosti u EU upravi i osigurava njihovu saglasnost sa pravilima za zaštitu podataka. Osim toga, ENZP daje savete Evropskoj komisiji, Evropskom parlamentu i Savetu o predlozima novih propisa i drugim pitanjima od važnosti za zaštitu podataka. ENZP takođe sarađuje sa drugim organima za zaštitu podataka kako bi se promovisala dosledna zaštita podataka širom Evrope.¹²¹

Zajedno sa osnovnim uslovom nezavisnosti, delokrug rada ESZP obuhvata:

- razvijanje i širenje sveobuhvatne vizije, razmišljanje u globalnim razmerama, kao i predlaganje konkretnih preporuka i praktičnih rešenja;
- davanje političkih smernica u cilju rešavanja novih i nepredviđenih izazova u oblasti zaštite podataka;
- rad na najvišim nivoima i uspostavljanje i održavanje delotvornih odnosa sa raznolikom zajednicom zainteresovanih strana u drugim institucijama EU, državama članicama, trećim zemljama, i drugim nacionalnim ili međunarodnim institucijama.¹²²

¹²¹ <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS> (pristupljeno 16. 3. 2017).

¹²² <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/cache/offonce#> (pristupljeno 17. 2. 2017).

Pravni okvir

Misija ENZP definisana je u Uredbi (EZ) br. 45/2001, gde je navedeno da ovo telo *ima za cilj da služi kao centar izvrsnosti za sprovođenje i jačanje zaštite podataka i standarda privatnosti u EU, kako u praksi tako i u zakonu.*

U Članovima 46. i 47. Uredbe (EZ) br. 45/2001 izričito je navedeno koja su ovlašćenja i dužnosti ENZP.

Nadležnosti

Nadležnosti ENZP obuhvataju nadzor nad telima i institucijama EU, inspekcijske nadzore i istražne postupke pokrenute na sopstvenu inicijativu – nadgledanje poštovanja propisa i prethodna procena rizika za operacije obrade nakon obavezujućeg obaveštenja – preporuke za implementaciju. On takođe postupa po žalbama koje podnose lica na koje se podaci odnose, koji smatraju da neka institucija ili telo EU ne postupa sa njihovim podacima na odgovarajući način, usvaja mišljenja i smernice o merama i administrativnim merama koje preduzima uprava EU, vodi registar zbirki podataka koje obrađuju tela i institucije EU i učestvuje u redovnim sastancima Mreže službenika za zaštitu podataka EU institucija i tela.¹²³

Što se tiče konsultacija za tela i institucije EU, ENZP daje savete o predlozima novih zakona i mekog prava, npr. proverava uticaj predloga na zaštitu podataka i privatnost. Osim toga, ENZP prati uticaj novih tehnologija na zaštitu podataka i privatnost. I na kraju, on interveniše u slučajevima pred Evropskim sudom pravde i Prvostepenim sudom.

ENZP usvaja predloge praktične politike, objavljuje Popis o godišnjim prioritetima, izdaje javna mišljenja i komentare o saopštenjima EK.

¹²³ <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/cache/offonce#> (pristupljeno 17. 2. 2017).

Ona obuhvata rad na posebnim pitanjima, kao što je tumačenje Direktive EU o zaštiti podataka, i strukturniju saradnju sa drugim organima za zaštitu podataka. Prevažadni cilj ENZP je da promoviše doslednost u zaštiti podataka o ličnosti širom EU.

ENZP takođe učestvuje u radu kako bi se obezbedila dobra zaštita podataka u trećem stubu EU, koji obuhvata policijsku i pravosudnu saradnju (ranije „treći stub EU“). To uključuje učestvovanje na nekim sastancima Zajedničkih nadzornih tela koja se bave informacionim sistemima u oblasti policije i pravosuđa. On je takođe i član Radne grupe 29 i Radne grupe za policiju i pravosuđe, koje je uspostavila Evropska konferencija za pružanje saveta u oblasti sprovođenja zakona.¹²⁴

Jedan od najvažnijih zadataka vezano za saradnju odnosi se na veliki IT sistem Eurodac¹²⁵, gde su odgovornosti za nadzor nad zaštitom podataka podeljene. Sistem se sastoji od nekoliko nacionalnih jedinica (shodno nacionalnom zakonu) i centralne jedinice (shodno Uredbi EU o zaštiti podataka). To, naravno, zahteva koordinisan pristup koji se razvija kroz dvogodišnje koordinacione sastanke koje organizuje ENZP.

Svake godine održavaju se dve velike konferencije o zaštiti podataka. Svakog proleća, Evropska konferencija¹²⁶ okupi službenike za zaštitu podataka iz nadležnih organa država članica EU i Saveta Evrope. Stručnjaci za zaštitu prava iz raznih oblasti, kako iz javnog tako i privatnog sektora, takođe se svakog proleća sastaju na Međunarodnoj konferenciji¹²⁷.

¹²⁴ <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/cache/offonce#> (pristupljeno 17. 2. 2017).

¹²⁵ <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Seurodac> (pristupljeno 17. 2. 2017).

¹²⁶ Nadležni organi za zaštitu podataka iz država članica EU i Saveta Evrope sastaju se na godišnjem nivou na prolećnoj konferenciji, gde razgovaraju o pitanjima od zajedničkog interesa i razmenjuju informacije i iskustva o različitim temama. ENZP aktivno doprinosi diskusijama. Konferencija se obično završava usvajanjem nekoliko važnih dokumenata.

¹²⁷ Godišnja međunarodna konferencija poverenika za zaštitu podataka i privatnosti okuplja, pored javnih službenika iz (inter)nacionalnih nadležnih organa i podnacionalnih nadležnih organa, i

ENZP daje mišljenje o „velikim podacima“ (*Big Data*). Mnogi evropski veliki IT sistemi stvoreni su sa ciljem da unaprede saradnju i razmenu informacija između nacionalnih nadležnih organa (i, u nekim slučajevima, tela Unije), npr. azil, vize, saradnja u sprovođenju zakona, pitanja u oblasti carine i otvorenog tržišta. Da pomenemo samo neke: Eurodac (otisci prstiju), Vizni informacioni sistem (VIS), Šengenski informacioni sistem (SIS), Carinski informacioni sistem (CIS) i Informacioni sistem unutrašnjeg tržišta (IMI).¹²⁸

Nadzor i sprovođenje

Jedan od glavnih zadataka Evropskog nadzornika za zaštitu podataka je da nadgleda obradu podataka o ličnosti od strane evropskih institucija i organa. Taj posao obavlja se kroz nekoliko različitih vrsta aktivnosti.

Veći deo se zasniva na obaveštenjima o operacijama obrade koji predstavljaju posebne rizike. Oni moraju biti prethodno provereni¹²⁹ od strane ENZP. Na osnovu činjenica koje mu se dostave, ENZP će ispitati obradu podataka o ličnosti u odnosu na Uredbu o zaštiti podataka (Uredba (EZ) 45/2001). U većini slučajeva, to dovodi do seta preporuka koje je potrebno da neka institucija ili telo sprovede kako bi se obezbedilo poštovanje propisa o zaštiti podataka.

druge stručnjake u ovoj oblasti. Ovaj događaj je veći od Evropske konferencije, ne samo u geografskom smislu, već i zbog toga što spaja predstavnike privrede i akademike. Međunarodna konferencija predstavlja priliku za zainteresovane strane u oblasti zaštite podataka u Evropi da se susretnu sa kolegama iz Kanade, Latinske Amerike, Australije, Novog Zelanda, Hong Konga, Japana i drugih jurisdikcija u azijsko-pacifičkom regionu. Diskutuje se o pitanjima od zajedničkog interesa, izazovima u budućnosti, i kako zajedno raditi i napredovati.

¹²⁸ <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS> (pristupljeno 16. 3. 2017).

¹²⁹ Član 27. stav 1. Uredbe (EZ) br. 45/2001 predviđa da svi „postupci obrade, koji zbog svoje prirode, obima ili svrhe, mogu predstavljati posebne rizike za prava i slobode lica na koja se podaci odnose“ podležu prethodnoj proveru Evropskog nadzornika za zaštitu podataka. Prethodne provere služe da se utvrdi da li uprava EU planira da obradi podatke o ličnosti u skladu sa Uredbom, ili da li je potrebno da se sistem unapredi sa stanovišta zaštite podataka. Više informacija na <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/priorchecking> (pristupljeno 17. 2. 2017).

ENZP usvaja mišljenja o administrativnim merama vezano za zaštitu podataka koja su usvojili evropske institucije i tela.

ESZP može da pokrene istražni postupak na sopstvenu inicijativu. Istražni postupci i inspekcijski nadzori su od suštinskog značaja za nadzorni organ, koji na taj način ima sredstvo za utvrđivanje činjenica, praćenje slučajeva i nadgledanje poštovanja propisa generalno.

Za praćenje poštovanja Uredbe (EZ) br. 45/2001, ENZP se u velikoj meri oslanja na službenike za zaštitu podataka (SZP) koji bi trebalo da budu imenovani u svakoj instituciji/telu. Pored bilateralnih sastanaka i kontakata sa SZP, ENZP takođe učestvuje u redovnim sastancima Mreže službenika za zaštitu podataka.

ENZP objavljuje tematske smernice¹³⁰ o ključnim pitanjima koja služe kao referenta dokumenta za evropsku upravu.

ENZP je u decembru 2010. godine usvojio predlog praktične politike pod naslovom „Praćenje i obezbeđivanje usaglašenosti sa Uredbom (EZ) 45/2001“¹³¹.

Prethodna procena rizika

ENZP proverava postupke obrade koji zbog svoje prirode, obima ili svrhe mogu predstavljati posebne rizike za prava i slobode lica na koje se podaci odnose:

- Obrada podataka o zdravstvenom stanju, o osumnjičenosti za izvršenje krivičnih dela, krivičnim delima, krivičnim presudama ili zaštitnim merama;

¹³⁰ <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines> (pristupljeno 17. 2. 2017).
¹³¹ Praćenje i obezbeđivanje usaglašenosti sa Uredbom (EZ) 45/2001, predlog praktične politike, Brisel, 13. decembar 2010, dostupno na: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_EN.pdf (pristupljeno 17. 2. 2017).

- Operacije obrade koje za cilj imaju procenu ličnih aspekata lica na koje se podaci odnose, uključujući njegovu sposobnost, efikasnost i ponašanje;
- Operacije obrade koje omogućavaju povezivanje koje nije predviđeno nacionalnim zakonodavstvima ili zakonodavstvom EU između podataka koji se obrađuju u različite svrhe;
- Operacije obrade u svrhu isključivanja pojedinaca iz prava, dobrobiti ili ugovora.

Institucije i tela dužna su da odmah obaveste ENZP o nameravanoj obradi, a ukoliko postoji sumnja dužni su da se konsultuju sa istom. ENZP može da zatraži i dodatne informacije. Ova institucija bi trebalo da svoje mišljenje dostavi u roku od 2, a najviše 4 meseca. Ukoliko to nije urađeno utoliko se smatra da je mišljenje pozitivno.

ENZP može takođe da daje predloge u slučaju da se obradom narušavaju odredbe Uredbe (EZ) br. 45/2001, i ukoliko rukovalac podataka, shodno tome, ne promeni operaciju obrade (Član 47. stav 1).

Žalbe lica na koje se podaci odnose

U slučaju žalbe lica na koje se podaci odnose da je došlo do povrede prava ENZP će primeniti postupak koji je predviđen u Članu 32. ENZP je nadležan da se bavi samo navodnim povredama vezanim za obradu podataka o ličnosti, a ne na druge oblike nepravilnog rada uprave, navodnim povredama prava od strane tela ili institucija Zajednice, a ne povrede od strane privatnih subjekata i nacionalnih nadležnih organa, pošto ENZP nije apelaciono telo i ne prihvata pojedinačne žalbe lica na koje se podaci odnose, ali svi zaposleni u EU mogu da se žale na „druge“. Takođe treba napomenuti da, na osnovu Memoranduma o razumevanju, podnosilac žalbe može da odabere da li će podneti žalbu ENZP ili Ombudsmanu (zaštitniku građana). Savetuje se, ali to nije obavezno, da se prvo kontaktira rukovalac podataka i/ili službenik za zaštitu podataka.¹³²

¹³² <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS> (pristupljeno 16. 3. 2017).

Žalba treba da bude u pisanom i elektronskom obliku, i da pruža dovoljno informacija i dokaza. ENZP zatim ispituje prihvatljivost žalbe, i ukoliko se ne dobije odgovor u roku od 6 meseci žalba se smatra odbačenom. Shodno tome, ENZP ne mora obavezno da odgovori na svaku žalbu, čime se štedi vreme, i ENZP može da potroši više vremena i energije na druge bitne stvari. Žalba treba da bude dovoljno osnovana, u smislu da nije očigledno beznačajna ili da je potrebna istraga koja bi zahtevala nesrazmerno velike napore.

ENZP može da donosi sledeće odluke: da da savet licu na koje se podaci odnose, upozori ili opomene rukovaoca podataka, izrekne zabranu obrade podataka ili prosledi slučaj ESP. Podnosilac žalbe može da zahteva da ENZP preispita odluku u roku od mesec dana od dana njenog donošenja. Podnosilac žalbe takođe ima pravo da podnese žalbu na odluku ESP.¹³³

Mišljenje 7/2015: Savladavanje izazova u vezi sa velikim podacima (*Big Data*)

Mišljenje predstavlja poziv za transparentnost, kontrolu korisnika, zaštitu podataka po principu ugrađene privatnosti i odgovornosti.¹³⁴

Veliki podaci su „praksa kombinovanja ogromnih količina informacija iz različitih izvora i njihova analiza, koristeći sofisticiranije algoritme u cilju poboljšanja donošenja odluke“. To nije samo prikupljanje i skladištenje velikih količina podataka, već i mogućnost da se ti podaci analiziraju i razumeju. Oni imaju veliki prediktivni potencijal, mogu da otkriju opšte trendove i korelacije, a mogu i da stvore obrasce razmišljanja, psihološke profile i omoguće procenu rizika.

¹³³ <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/cache/offonce#> (pristupljeno 17. 2. 2017).

¹³⁴ Mišljenje ENZP 7/2015, *Meeting the Challenges of Big Data: A Call for transparency, user control, data protection by design and accountability*, novembar 2015.

Oglašivači ih koriste za određivanje cene prilagođene pojedincu i ciljanje ranjivih potrošača, osiguravajuća društva za procenu zdravstvenog i životnog rizika, poslodavci u postupku selekcije kako bi pronašli „kandidata“ koji im najviše odgovara, istražitelji i obavешtajne agencije za tendenciju da se poćini zloćin, krivićno delo ili teroristićki akt, naućnici za istraćivanje, potrošaći – npr. TripAdvisor i slićne platforme za ocenjivanje i upućivanje, ali i banke za procenu kreditnog rizika.

Rizici su upotreba u neutvrđene buduće svrhe (nedostatak transparentnosti), gde sada anonimni podaci to ne moraju biti u budućnosti (deljenje podataka putem javnih društvenih medija), informaciona neravnoteća (diskriminacija), relevantnost i taćnost predviđanja i zakljućaka („Mi smo ono što podaci kaću o nama“), društvena, kulturna segregacija i iskljućenje, pravljenje stereotipa („Ćovek je poznat po društvu koje ima“), stvaranje *filtriranih mehurića* ili lićnih *eho-komora*, ima negativan efekat na inovacije, kreativnost, slobodu izraćavanja, okupljanja i udrućivanja jer obeshrabruje spontanost i podstiće konformizam.

U svetu koji je svakim danom sve viće personalizovan, algoritmi nagađaju koje informacije bi svako od nas ćeleo da vidi na osnovu toga što zna o nama (na primer, naće lokacije, istorije pretraćivanja, ponaćanja i kupovine). Svaka informacija koju primimo filtrira se na sve sloćenije i nejasnije naćine. Postoji opasnost da ćemo sve manje biti u prilici da naićdemo na informacije koje će preispitivati naća postojećća gledića. Sve viće ćemo biti efikasno izolovani u sopstvenim kulturnim i ideoloćkim „mehurićima“, i odvojeni od ostatka društva. Naći vidici bi trebalo da se ćire u informacionom društvu, ali veliki podaci – profilisanje – imaju upravo suprotan efekat – sućavaju naću perspektivu, što ćini da verujemo da postoje samo ljudi koji misle kao mi, rade i vole iste stvari kao mi.¹³⁵

¹³⁵ ENZP, Mićljenje 7/2015, dostupno na: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf (pristupljeno 14. 3. 2017).

Podaci nisu transparentni pošto obrađeni podaci ne predstavljaju samo prikupljene, već i tumačene posmatranjem i analizom, i zbog toga što se podaci prikupljaju iz različitih izvora. Rukovaoci podataka bi trebalo da otkriju logiku primenjenu u analitici velikih podataka i donošenju odluke, kao i da zaštite poverljivost ili poslovne tajne pomoću alata za zaštitu intelektualne svojine. Oni mogu da obelodane informacije proaktivno u „slojevitom“ obaveštenju, ali bi te informacije trebalo da budu na jasnom i jednostavnom jeziku, prilagođene odgovarajućoj publici, i takođe da obelodane izvore podataka. Gde postoji dvosmislenost u politikama trebalo bi da se tumače u korist lica na koje se podaci odnose.¹³⁶

Slojevito (postepeno) obaveštenje podrazumeva da se lice na koje se podaci odnose obaveštava o obradi svojih podataka korak po korak. To podrazumeva dostavljanje pojedincu bitne informacije o obradi u trenucima kada isti treba da donese odluku na osnovu informacija (na primer, pojedinac bi trebalo da zna da li će skinuta aplikacija imati pristup podacima o njegovoj lokaciji pre nego što donese odluku da li da je instalira). A zatim dostavljanje daljih informacija u drugim formatima, na primer putem detaljnijih informacija na internet stranici. U suštini, ne bi trebalo zatrpavati pojedinca dugim nečitljivim obaveštenjima o privatnosti, već davati konkretne informacije kada je to potrebno. Ne davanje obaveštenja o privatnostima tipa „za advokate od advokata“.

Lice na koje se podaci odnose trebalo bi da može da kontroliše svoje podatke davanjem izričitog prethodnog pristanka ili implicitnog pristanka sa opcijom napuštanja (opt-out). Ono takođe treba da ima pravo da pristupi i ispravi svoje podatke, koje proističe iz Člana 8. stav 2. Povelje o osnovnim pravima EU i Člana 12. Direktive 95/46/EZ. U ovom smislu, važan je pojam prenosivosti podataka.¹³⁷

¹³⁶ ENZP, Mišljenje 7/2015, dostupno na: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf (pristupljeno 14. 3. 2017).

¹³⁷ Isto.

2.4. AGENCIJA ZA OSNOVNA PRAVA EVROPSKE UNIJE

Agencija za osnovna prava Evropske unije (FRA) osnovana je 2007. kao agencija Evropske unije sa specifičnim zadatkom pružanja nezavisnih saveta zasnovanih na dokazima u oblasti osnovnih prava. Ova Agencija je centar EU za stručnost u oblasti osnovnih prava. Takođe je jedna od decentralizovanih agencija EU. Ove agencije uspostavljene su radi pružanja stručnih saveta institucijama EU i državama članicama po raznim pitanjima.

Kroz prikupljanje i analizu podataka u Evropskoj uniji, Agencija za osnovna prava pomaže institucijama Evropske unije, kao i državama članicama u razumevanju i prevazilaženju problema. Zahvaljujući partnerstvu sa institucijama Evropske unije, njenim državama članicama i drugim organizacijama na međunarodnom, evropskom i nacionalnom nivou, Agencija za osnovna prava EU igra značajnu ulogu u omogućavanju sprovođenja osnovnih prava u praksi za sve građane Evropske unije.¹³⁸

Agencija zapošljava 90 službenika, uključujući pravne eksperte, stručnjake političkih i društvenih nauka, statističare i stručnjake za komunikaciju i umrežavanje. Njihovim radom rukovodi Upravni odbor Agencije. Upravni odbor je zadužen za utvrđivanje prioriteta u radu, odobravanje budžeta i praćenje rada Agencije. Članove Upravnog odbora čine nezavisni stručnjaci, po jedan iz svake države članice, dva predstavnika Evropske komisije i jedan nezavisan stručnjak koga imenuje Savet Evrope.

Agencija za osnovna prava je naslednik nekadašnjeg Evropskog centra za praćenje rasizma i ksenofobije (EUMC), ali ima mnogo šira ovlašćenja da pruža savete zasnovane na dokazima o širokom spektru osnovnih prava, u skladu sa Evropskom poveljom o osnovnim pravima. EUMC, koji je osnovan u Beču kao nezavisno telo Evropske

¹³⁸ <http://fra.europa.eu/en/about-fra> (pristupljeno 2. 3. 2017).

unije 1997, počeo je sa radom 1998, a prestao 28. februara 2007. godine.¹³⁹

Zadaci Agencije za osnovna prava obavljaju se kroz konsultaciju i saradnju sa partnerima. Agencija održava posebno bliske veze sa:

- Evropskom komisijom, Evropskim parlamentom i Savetom Evropske unije;
- drugim međunarodnim organizacijama kao što su Savet Evrope, Ujedinjene nacije (UN) i Organizacija za evropsku bezbednost i saradnju (OEBS);
- vladama, organizacijama civilnog društva, akademskim institucijama, telima za promovisanje ravnopravnosti i nacionalnim institucijama za ljudska prava.

Nadležnosti

Agencija za osnovna prava istražuje i prikuplja podatke, pruža pomoć i daje stručno mišljenje, i podiže svest.

Agencija za osnovna prava EU ima zadatak da prikuplja „objektivne, pouzdane i uporedive“ informacije i podatke. Ona sprovodi istraživanje o raznim temama širom Evropske unije umesto da nadgleda ili ocenjuje pojedinačne države članice.

Agencija za osnovna prava EU pruža pomoć i daje stručno mišljenje institucijama Evropske unije i državama članicama kako bi im pružila podršku u „punom poštovanju osnovnih prava“ prilikom izrade i sprovođenja zakona Evropske unije.

Agencija za osnovna prava EU nastoji da poboljša stanje na terenu. Ona to čini i kroz podizanje svesti o osnovnim pravima u javnosti i među određenim profesijama koje igraju važnu ulogu u ostvarivanju

¹³⁹ <http://fra.europa.eu/en/about-fra/who-we-are> (pristupljeno 1. 3. 2017).

naših prava ili imaju uticaj na njih kao što su nastavnici, stručnjaci u oblasti medija, policajci i pravnici.¹⁴⁰

1) Velika istraživanja

- Prvo EU istraživanje o iskustvima o diskriminaciji i viktimizaciji imigranata i manjina¹⁴¹ (EU – MIDIS): 23.500 ispitanika iz grupa imigranata i pripadnika nacionalnih manjina. Naknadno istraživanje je trenutno u toku.
- Najveće istraživanje ikada sprovedeno o rodno zasnovanom nasilju nad ženama u svim državama članicama EU¹⁴²: 42.000 žena.
- Najveće istraživanje na nivou EU o zločinima iz mržnje i diskriminaciji prema lezbejkama, gejevima, biseksualcima i transrodnim osobama¹⁴³: 93.000 pripadnika LGBT populacije.
- Istraživanje o uslovima života i stanju diskriminacije među Romima¹⁴⁴: 85.000 osoba.
- Istraživanje o antisemitizmu¹⁴⁵: 6.000 Jevreja.
- Istraživanje na nivou EU o osnovnim pravima¹⁴⁶ među opštom populacijom o njihovim gledištima i iskustvima: u toku.

2) Komparativna pravna ili sociološka istraživanja

- Usluge podrške žrtvama u EU: pregled i ocena prava žrtava u praksi;
- Zločini iz mržnje u Evropskoj uniji¹⁴⁷;

¹⁴⁰ <http://fra.europa.eu/en/about-fra> (pristupljeno 2. 3. 2017).

¹⁴¹ <http://fra.europa.eu/en/survey/2012/eu-midis-european-union-minorities-and-discrimination-survey> (pristupljeno 1. 3. 2017).

¹⁴² <http://fra.europa.eu/en/publications-and-resources/data-and-maps/survey-data-explorer-violence-against-women-survey> (pristupljeno 2. 3. 2017).

¹⁴³ <http://fra.europa.eu/DVS/DVT/lgbt.php> (pristupljeno 1. 3. 2017).

¹⁴⁴ <http://fra.europa.eu/DVS/DVT/roma.php> (pristupljeno 1. 3. 2017).

¹⁴⁵ <http://fra.europa.eu/en/publication/2013/discrimination-and-hate-crime-against-jews-eu-member-states-experiences-and> (pristupljeno 1. 3. 2017).

¹⁴⁶ <http://fra.europa.eu/en/project/2015/fundamental-rights-survey> (pristupljeno 1. 3. 2017).

¹⁴⁷ <http://fra.europa.eu/en/theme/hate-crime> (pristupljeno 13. 2. 2017).

- Pravni lekovi za zaštitu podataka¹⁴⁸ i nadzor obaveštajnih službi;
- Teška eksploatacija na radu;
- Dostupnost pravdi¹⁴⁹;
- Deca i pravda¹⁵⁰;
- Osnovna prava migranata koji nezakonito borave u EU¹⁵¹;
- Osnovna prava osoba sa invaliditetom¹⁵².

3) Priručnici za pravnike

U ovim priručnicima predstavljeno je zakonodavstvo i studije slučaja EU na jedan dostupan način. Obuhvaćene su sledeće teme:

- azil, granice i imigracija¹⁵³;
- prava deteta¹⁵⁴;
- zaštita podataka;
- nediskriminacija¹⁵⁵.

Agencija za osnovna prava objavila je dva priručnika u vezi sa zaštitom podataka, i to „Dostupnost pravnih lekova koji se odnose na zaštitu podataka u državama članicama EU“ i „Priručnik o evropskom pravu u oblasti zaštite podataka“.¹⁵⁶

¹⁴⁸ <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states> (pristupljeno 6. 3. 2017).

¹⁴⁹ <http://fra.europa.eu/en/theme/access-justice> (pristupljeno 13. 2. 2017).

¹⁵⁰ <http://fra.europa.eu/en/project/2012/children-and-justice> (pristupljeno 13. 2. 2017).

¹⁵¹ <http://fra.europa.eu/en/publication/2012/fundamental-rights-migrants-irregular-situation-european-union> (pristupljeno 15. 2. 2017).

¹⁵² <http://fra.europa.eu/en/theme/people-disabilities> (pristupljeno 13. 2. 2017).

¹⁵³ Handbook on European law relating to asylum, borders and immigration, available at: <http://fra.europa.eu/en/publication/2013/handbook-european-law-relating-asylum-borders-and-immigration> (pristupljeno 1. 3. 2017).

¹⁵⁴ <http://fra.europa.eu/en/publication/2015/handbook-european-law-child-rights> (pristupljeno 5. 3. 2017).

¹⁵⁵ <http://fra.europa.eu/en/publication/2011/handbook-european-non-discrimination-law> (pristupljeno 6. 3. 2017).

¹⁵⁶ [http://fra.europa.eu/en/publications-and-resources/publications?title=law&field_fra_publication_type_tid_i18n\[0\]=88](http://fra.europa.eu/en/publications-and-resources/publications?title=law&field_fra_publication_type_tid_i18n[0]=88) (pristupljeno 1. 3. 2017).

Delokrug rada

Cilj, obim i zadaci Agencije za osnovna prava EU navedeni su u Uredbi Saveta (EZ) br. 168/2007, kojom se uspostavlja Agencija za osnovna prava Evropske unije.

U Članu 2. Uredbe Saveta (EZ) br. 168/2007 stoji:

Cilj Agencije je da pruži relevantnim institucijama, telima, kancelarijama i agencijama Zajednice i njenim državama članicama, stručnu pomoć u oblasti osnovnih prava prilikom sprovođenja prava Zajednice, kako bi im pomogla u preduzimanju mera ili formulisanju odgovarajućih aktivnosti u okviru svojih nadležnosti, a sve u cilju potpunog poštovanja osnovnih prava.¹⁵⁷

Evropski parlament, Savet EU i Evropska komisija mogu da zatraže istraživanje ili mišljenje o specifičnom pitanju, van programa rada Agencije, uključujući i period tokom zakonodavnih postupaka. Države članice mogu da zatraže uporedne podatke i informacije od Agencije za osnovna prava kako bi se informisale o razvoju nacionalnih politika.

Tematske oblasti rada Agencije određuju se petogodišnjim višegodišnjim okvirom. 11. marta 2013. godine Savet za pravosuđe i unutrašnja pitanja EU, na predlog EK i nakon konsultacija sa Evropskim parlamentom, usvojio je trenutno važeći Višegodišnji okvir Agencije.¹⁵⁸

U Odluci Saveta navedeno je da će rad Agencije obuhvatiti sledećih devet oblasti:

- a) dostupnost pravdi;
- b) žrtve zločina, uključujući i nadoknadu štete žrtvama;
- c) informaciono društvo, a naročito poštovanje privatnosti i zaštita podataka o ličnosti;
- d) integracija Roma;

¹⁵⁷ Uredba Saveta (EK) br. 168/2007, od 15. februara 2007, kojom se osniva Agencija Evropske unije za osnovna prava, Službeni list L53/1.

¹⁵⁸ <http://fra.europa.eu/en/about-fra> (pristupljeno 2. 3. 2017).

- e) pravosudna saradnja, osim u krivičnim stvarima;
- f) prava deteta;
- g) diskriminacija na osnovu pola, rase, boje, etničkog ili socijalnog porekla, genetskih osobina, jezika, vere ili verovanja, političkog uverenja ili nekog drugog mišljenja, pripadanja nacionalnoj manjini, vlasništva, rođenja, invaliditeta, starosti ili seksualne orijentacije;
- h) imigracija i integracija migranata, vizna i granična kontrola, i azil;
- i) rasizam, ksenofobija i povezana netolerancija.

Okvir se sprovodi kao komplementarnost radu drugih EU tela, Saveta Evrope i ostalih međunarodnih organizacija koje se bave ljudskim pravima.

Trenutno važeći višegodišnji okvir ističe 31. decembra 2017. godine i biće zamenjen novom Odlukom Saveta.¹⁵⁹

¹⁵⁹ Spisak primera dostupan je na: <http://fra.europa.eu/en/about-fra/how-we-do-it/how-our-work-is-used> (pristupljeno 1. 3. 2017).

2.5. EVROPSKI SUD PRAVDE

Evropski sud pravde (ESP) tumači pravo EU kako bi se osigurala njegova ujednačena primena u svim zemljama članicama EU, osigurava da zemlje članice i institucije EU poštuju pravo EU i rešava pravne sporove između vlada zemalja članica i institucija EU. U izvesnim okolnostima pojedinci, privredni subjekti ili organizacije mogu se obratiti Sudu kako bi pokrenuli postupak protiv neke institucije EU, ako smatraju da je povredila njihova prava na neki način.¹⁶⁰

ESP čini po jedan sudija iz svake zemlje članice EU i 11 opštih pravobranilaca. Opšti sud čini 47 sudija. Taj broj će se 2019. godine povećati na 56 (po dvojica sudija iz svake države članice EU). ESP je osnovan 1952. godine sa sedištem u Luksemburgu.

ESP donosi odluke u postupcima koji su pokrenuti pred njim. Pet najčešćih vrsta postupaka:

- Tumačenje prava (postupak za rešavanje prethodnog pitanja) – domaći sudovi zemalja EU dužni su da osiguraju pravilnu primenu prava EU, ali sudovi u različitim zemljama mogu ga različito tumačiti. Ako domaći sud ima nedoumice povezane s tumačenjem ili valjanošću prava EU može se obratiti Sudu radi pojašnjenja. Isti mehanizam se može primeniti da bi se utvrdilo da li su domaći zakon ili praksa usklađeni sa pravom EU.
- Primena prava (postupci zbog povrede prava) – postupci ove vrste pokreću se protiv nacionalnih vlada ako ne postupaju u skladu sa pravom EU. Mogu ih pokrenuti Evropska komisija ili druga država članica EU. Ako se utvrdi da je određena država članica pogrešila, ona mora odmah da preduzme mere da ispravi pogrešku, u protivnom se može pokrenuti drugi postupak, u kojem se toj državi može izreći novčana kazna.

¹⁶⁰ https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (pristupljeno 19. 3. 2017).

- Poništenje pravnih akata EU (postupci za poništenje) – ako se smatra da se određenim aktom EU krše ugovori o EU ili osnovna prava, vlada države članice EU, Savet EU, Evropska komisija ili (u nekim slučajevima) Evropski parlament od Suda mogu zahtevati da poništi taj akt. I fizička lica mogu od Suda zahtevati da poništi određeni akt EU koji se direktno odnosi na njih.
- Osiguravanje delovanja EU (tužbe zbog propusta) – Parlament, Savet i Komisija dužni su da donose određene odluke u određenim okolnostima. Ako to ne učine, vlade država članica EU, druge institucije EU ili (u određenim okolnostima) pojedinci ili privredni subjekti mogu se obratiti Sudu.
- Kažnjavanje institucija EU (postupci za naknadu štete) – svi pojedinci ili privredni subjekti čiji su interesi oštećeni zbog postupanja ili nepostupanja EU ili njenih kadrova mogu da pokrenu postupak protiv njih pred Sudom.¹⁶¹

Sastav

ESP čine dva suda:

- Sud pravde – odlučuje po zahtevima za rešavanje prethodnog pitanja koje podnose domaći sudovi, u određenim postupcima za poništenje i o žalbi.
- Opšti sud – odlučuje u postupcima za poništenje koje su pokrenuli pojedinci, privredni subjekti, i, u nekim slučajevima, vlada države članice EU. To u praksi znači da ovaj Sud uglavnom postupuje u predmetima povezanim sa zakonodavstvom o konkurenciji, dodeli državne pomoći, trgovini, poljoprivredi i žigovima.

Sudije i opšte pravobranioce sporazumno imenuju nacionalne vlade na mandat od 6 godina, sa mogućnošću reizbora. U oba suda sudije biraju predsednika na mandat od 3 godine, sa mogućnošću reizbora.

¹⁶¹ https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (pristupljeno 19. 3. 2017).

Postupak

U Sudu pravde se svaki predmet dodeljuje jednom sudiji („sudija izvestilac“) i jednom opštem pravobraniocu. Predmeti se obrađuju u dve faze:

- Pisana faza
 - o Stranke Sudu podnose pisane izjave – izjave mogu podneti i državni organi, institucije EU, a ponekad i fizička lica.
 - o Sudija izvestilac sastavlja sažetak od tih izjava, o kojem se raspravlja na opštoj sednici Suda, gde se odlučuje:
 - o broju sudija koji će postupati u predmetu: 3, 5 ili 15 sudija (celi Sud), u zavisnosti od značaja i složenosti predmeta. U većini predmeta postupa 5 sudija, i veoma retko se dešava da celi Sud postupa u predmetu;
 - da li je potrebno održati ročište (usmena faza) i da li je potrebno pribaviti mišljenje opšteg pravobranioaca.
- Usmena faza – javna rasprava
 - o Advokati obe strane mogu da izlože predmet sudijama i opštem pravobraniocu, koji mogu da ih ispituju.
 - o Ako Sud odluči da je neophodno mišljenje opšteg pravobranioaca, isti ga podnosi nekoliko sedmica posle rasprave.
 - o Nakon toga sudije raspravljaju o predmetu i donose presudu.
- Postupak pred Opštim sudom je sličan, ali u većini predmeta postupaju tri sudije bez opštih pravobranilaca.¹⁶²

¹⁶²

https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (pristupljeno 5. 3. 2017).

Presuda u spojenim predmetima C-293/12 i C-594/12
(*Digital Rights Ireland* i *Seitlinger* i ostali) od 8. aprila 2014.¹⁶³

Upućivanje predmeta na rešavanje prethodnog pitanja omogućava sudovima i tribunalima država članica, u sporovima koji se vode pred njima, da upute pitanja Sudu pravde u vezi sa tumačenjem prava Evropske unije ili valjanošću odredaba akta Evropske unije. Sud pravde ne odlučuje o ishodu spora. Domaći sud ili tribunal postupaju u predmetu u skladu sa odlukom Suda, koja je obavezujuća i za druge domaće sudove ili tribunale pred kojima se pojavi slično pitanje.

U ovom slučaju, Sud pravde je Direktivu o zadržavanju podataka proglasio nevažećom, zato što se u velikom stepenu i prilično ozbiljno meša u vršenje osnovnih ljudskih prava na poštovanje privatnog života i zaštitu podataka o ličnosti, a da to mešanje nije ograničeno na ono što je striktno neophodno.¹⁶⁴

Osnovni cilj Direktive o zadržavanju podataka¹⁶⁵ bio je usaglašavanje odredaba propisa država članica koje se odnose na obavezu zadržavanja određenih podataka koje skupljaju ili obrađuju pružaoци elektronskih komunikacionih usluga ili javnih komunikacionih mreža. Cilj joj je stoga bio da osigura da ti podaci budu dostupni radi sprečavanja, istrage, otkrivanja i gonjenja teških krivičnih dela, kao što su organizovani kriminal i terorizam. Prema tome, Direktivom je bilo predviđeno da gorenavedeni provajderi moraju da zadrže podatke o sadržaju i lokaciji, kao i druge podatke neophodne za identifikaciju pretplatnika ili korisnika usluga. Nasuprot tome, nije dozvoljavala zadržavanje sadržaja elektronske komunikacije ili

¹⁶³ <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN> (pristupljeno 5. 3. 2017).

¹⁶⁴ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (pristupljeno 18. 3. 2017).

¹⁶⁵ Direktiva 2006/24/EZ.

informacija do kojih se dolazilo korišćenjem elektronskih komunikacionih mreža.

Visoki sud (Irska) i *Verfassungsgerichtshof* (Ustavni sud, Austrija) tražili su od Suda pravde da se izjasni o pravnoj valjanosti Direktive, uzimajući u obzir Povelju Evropske unije o osnovnim pravima, tačnije pravo na poštovanje privatnog života i pravo na zaštitu podataka o ličnosti. Visoki sud je rešavao u sporu između irske kompanije *Digital Rights Ireland* i irskih ograna vlasti u pogledu zakonitosti domaćih mera u vezi sa zadržavanjem podataka u vezi sa elektronskim komunikacijama. Pred *Verfassungsgerichtshof* je bilo nekoliko ustavnih tužbi koje su podneli *Kärntner Landesregierung* (Vlada pokrajine Koruške) i Seitlinger, Tschohl i 11.128 podnosilaca predstavke. Predmet tih tužbi bilo je proglašenje nevažećim odredaba domaćeg zakona kojim je direktiva prenetu u austrijsko pravo.¹⁶⁶

Sud je prvo primetio da su podaci za koje postoji obaveza zadržavanja omogućavali, naročito, (1) identifikaciju lica sa kojim je pretplatnik ili registrovani korisnik komunicirao, kao i sredstva kojim je komunikacija obavljena, (2) identifikaciju vremena komunikacije, kao i mesta na kome je komunikacija obavljena, i (3) utvrđivanje učestalosti komunikacije između korisnika i određenih lica tokom određenog vremenskog perioda. Ti podaci, uzeti zajedno, mogu da obezbede veoma precizne informacije o privatnom životu lica čiji se podaci zadržavaju, kao što su informacije o svakodnevnim navikama, mestu prebivališta ili boravka, svakodnevnom ili drugom kretanju, obavljenim aktivnostima, društvenim odnosima i društvenim okruženjima u kojima su se te osobe kretale.

Sud je zauzeo stav da je, zahtevom da se vrši zadržavanje navedenih podataka i omogućavanje nadležnim organima država da pristupe zadržanim podacima, Direktiva omogućila naročito teško mešanje

¹⁶⁶ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (pristupljeno 18. 3. 2017).

u osnovno pravo na poštovanje privatnog života i pravo na zaštitu podataka o ličnosti.

Nadalje, postojala je verovatnoća da se, usled činjenice da su se podaci zadržavali i naknadno koristili bez prethodnog obaveštavanja pretplatnika ili registrovanog korisnika usluga, kod dotičnih lica stvori osećaj da su njihovi životi predmet konstantnog nadzora.¹⁶⁷

Sud je zatim ispitivao da li se takvo zadiranje u osnovna prava može smatrati opravdanim.

Sud je naveo da zadržavanje podataka koje je zahtevala Direktiva nije bilo takvo da bi povredilo suštinu osnovnih prava na poštovanje privatnog života i na zaštitu podataka o ličnosti. Direktiva nije dozvoljavala uvid u sadržaj elektronske komunikacije kao takav i pružaoci usluga ili mreže morali su da poštuju određena načela zaštite i sigurnosti podataka.

Štaviše, zadržavanje podataka sa ciljem da se oni potencijalno ustupe nadležnim državnim organima stvarno jeste bilo u skladu sa ciljem od opšteg interesa – borba protiv teškog kriminala i, na posletku, očuvanje javne bezbednosti.

Međutim, Sud je smatrao da usvajanjem Direktive o zadržavanju podataka zakonodavni organi Evropske unije jesu prekoračili ograničenja koja nameće princip proporcionalnosti.

U tom kontekstu, Sud je smatrao da je, s obzirom na, sa jedne strane, važnu ulogu koju zaštita podataka o ličnosti ima u odnosu na osnovno pravo na poštovanje privatnog života, i, sa druge, stepen i težinu zadiranja u to pravo koje sadrži Direktiva, diskreciono pravo EU zakonodavca smanjeno tako da je potrebno sprovesti strogo preispitivanje tog prava.¹⁶⁸

¹⁶⁷ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (pristupljeno 18. 3. 2017).

¹⁶⁸ Ibid.

Iako je zadržavanje podataka koje je zahtevala Direktiva možda primereno za ostvarivanje cilja iste, nisu bila nametnuta odgovarajuća ograničenja primerena stepenu i težini mešanja Direktive u osnovna prava, kako bi se osiguralo da je to mešanje u granicama onog što je striktno neophodno.

Kao prvo, direktiva je obuhvatala, na uopšten način, sva lica, sva sredstva elektronske komunikacije i sve podatke o prometu bez ikakvog razlikovanja, ograničenja ili izuzetaka u smislu ciljeva borbe protiv teškog kriminala.

Kao drugo, Direktiva nije predviđala nikakav objektivni kriterijum koji bi nadležnim državnim organima omogućio pristup podacima i korišćenje podataka isključivo u svrhu sprečavanja, otkrivanja ili gonjenja za krivična dela, koja se mogu, imajući u vidu stepen i težinu mešanja u vršenje predmetnih osnovnih prava, smatrati dovoljno teškim da opravdaju takvo mešanje. Baš nasuprot, Direktiva je sadržala opšte upućivanje na „teško krivično delo“ koje svaka država članica definiše u svom domaćem zakonodavstvu. Pored toga, Direktiva nije predviđala materijalne ni proceduralne uslove pod kojima su nadležni državni organi mogli da pristupe podacima i da ih nakon toga koriste. Pristup podacima nije zavisio od prethodno pribavljenog odobrenja suda ili nezavisnog administrativnog tela.¹⁶⁹

Kao treće, kada je reč o periodu zadržavanja podataka, Direktiva je nametala period koji nije bio kraći od šest meseci, a da se pritom nije vršila nikakva kategorizacija podataka u pogledu lica na koje se odnose ili njihove eventualne opravdanosti za cilj kome se teži. Štaviše, minimalni period zadržavanja bio je šest meseci a maksimalni 24 meseca, a da pritom nije bilo bliže određeno da se period zadržavanja mora definisati na osnovu objektivnih kriterijuma kako bi se osiguralo da je ograničen na ono što je najnužnije.

¹⁶⁹ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (pristupljeno 18. 3. 2017).

Sud je takođe utvrdio da Direktiva nije predviđala dovoljno zaštitnih mera za osiguranje efektivne zaštite podataka od rizika od zloupotrebe i od svakog nezakonitog pristupa ili korišćenja podataka. Napomenuo je, *inter alia*, da je Direktiva dopuštala da pružaoci usluga uzimaju u obzir ekonomska razmatranja prilikom utvrđivanja nivoa zaštite koju primenjuju (a naročito kada se radi o troškovima primene bezbednosnih mera) i da nije osiguravala nepovratno uništenje podataka po isteku perioda njihovog zadržavanja.

Na kraju, Sud je naveo da Direktiva nije propisivala obavezu da se predmetni podaci zadržavaju na području EU. Stoga, Direktiva nije u potpunosti osiguravala nadzor nezavisnog organa nad ispunjenošću zahteva u pogledu zaštite i sigurnosti, kao što se to izričito zahteva Poveljom. Takav nadzor, izvršen na osnovu prava EU, predstavlja suštinski element zaštite lica u pogledu obrade podataka o ličnosti.¹⁷⁰

Presuda u predmetu C-131/12 (*Google Spain SL, Google Inc. protiv Agencia Española de Protección de Datos, Mario Costeja González*) od 13. maja 2014.¹⁷¹

ESP je operatora internet pretraživača proglasio odgovornim za obradu podataka o ličnosti koji su se pojavljivali na internet stranicama koje su objavljivala treća lica.

Prema tome, ako se, nakon pretrage imena nekog lica, u listi rezultata pojavi link ka internet stranici koja sadrži podatke o predmetnom licu, lice na koga se podaci odnose može se direktno obratiti operatoru i, ako operator ne odobri njegov zahtev, pokrene postupak pred nadležnim organima radi pribavljanja, pod određenim uslovima, naloga za brisanje tog linka sa liste rezultata.

¹⁷⁰ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (pristupljeno 5. 3. 2017).

¹⁷¹ <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&dclang=EN&mode=lst&dir=&occ=first&part=1&cid=885051> (pristupljeno 7. 3. 2017).

Direktiva EU¹⁷² ima za cilj zaštitu osnovnih prava i sloboda fizičkih lica (pravo na privatnost) u vezi sa obradom podataka o ličnosti, kao i uklanjanje prepreka za slobodan protok takvih podataka.

2010. godine, Mario Costeja González, državljaniin Španije, podneo je *Agencia Española de Protección de Datos* (španska Agencija za zaštitu podataka, AEPD) žalbu protiv *La Vanguardia Ediciones SL* (izdavač dnevnih novina velikog tiraža, naročito u Kataloniji) i protiv *Google Spain and Google Inc.* Costeja González je istakao da bi internet korisnik koji unese njegovo ime u internet pretraživač *Google group-e* (Google pretraga) dobijao listu rezultata pretrage u kojoj su bile prikazane dve stranice dnevnih novina *La Vanguardia*, od januara i marta 1998. godine. Na tim stranicama se nalazio oglas za javnu prodaju nekretnina koja je bila organizovana nakon postupka izvršenja na pokretnim stvarima radi namirenja potraživanja za socijalno osiguranje – socijalnog osiguranja Costeja González.¹⁷³

Tom žalbom Costeja González je tražio, sa jedne strane, da se listu *La Vanguardia* naloži brisanje ili izmena predmetnih stranica (kako se na njima više ne bi pojavljivali njegovi podaci o ličnosti) ili da list primeni određene alate internet pretraživača radi zaštite tih podataka. Sa druge strane, tražio je da se kompaniji *Google Spain* ili *Google Inc.* naloži da obriše ili prikrije njegove podatke o ličnosti kako se oni više ne bi pojavljivali u rezultatima pretrage i linkovima ka listu *La Vanguardia*. Costeja González je u tom kontekstu naveo da je postupak izvršenja nad pokretnim stvarima, u kome je on bio dužnik, okončan u potpunosti pre nekoliko godina i da je od tada upućivanje na taj postupak lišeno svake relevantnosti.

AEPD je odbila žalbu u delu koji se odnosi na list *La Vanguardia*, i ocenila da je to što je list objavio predmetne informacije zakonski opravdano. Sa druge strane, žalba je usvojena u delu koji se odnosi

¹⁷² Direktiva 95/46/EZ.

¹⁷³ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (pristupljeno 5. 3. 2017).

na *Google Spain* i *Google Inc.* *AEPD* je naložila tim dvema kompanijama da preduzmu potrebne mere za brisanje podataka iz indeksa i onemogućavanje pristupa tim podacima u budućnosti. *Google Spain* i *Google Inc.* su pokrenule dva odvojena postupka pred sudom *Audiencia Nacional* (Nacionalni visoki sud, Španija), sa zahtevom da se odluka *AEPD*-a poništi. U tom kontekstu je navedeni španski sud uputio niz pitanja Sudu pravde.

Sud pravde je, kao prvo, utvrdio da automatizovanom, stalnom i sistematskom pretragom interneta radi pronalaženja informacija objavljenih na njemu, pretraživač operatora „prikuplja“ podatke u smislu navedene Direktive. Osim toga, Sud smatra da operator „vraća“, „snima“ i „organizuje“ podatke u okviru svojih programa indeksiranja a zatim ih „pohranjuje“ na svojim serverima i, u određenim slučajevima, „otkriva“ i „stavlja na raspolaganje“ korisnicima u obliku listi rezultata pretrage. Imajući u vidu izričita i безусловna upućivanja na te operacije u direktivi, one se moraju klasifikovati kao „obrađ“ iako ih operator pretraživača jednako primenjuje i na druge vrste informacija koje nisu podaci o ličnosti. Sud je takođe istakao da su se operacije navedene u Direktivi morale klasifikovati kao obrada čak i kada su se isključivo odnosile na materijal koji je u identičnom obliku već bio objavljen u sredstvima javnog informisanja. Posledica opšteg odstupanja od primene Direktive bi u takvom slučaju bila gubitak dejstva te Direktive.¹⁷⁴

Osim toga, Sud je dalje utvrdio da je operator pretraživača bio „rukovalac podataka“ u toj obradi, u smislu Direktive, imajući u vidu da je operator određivao svrhu i način obrade. Sud je u tom smislu istakao da je, u meri u kojoj se ta aktivnost pretraživača nadovezivala na aktivnost objavljiivača internet stranice i mogla znatno da utiče na osnovna prava na privatnost i zaštitu podataka o ličnosti, operator pretraživača morao da u okviru svojih odgovornosti, nadležnosti i mogućnosti osigura da ta aktivnost zadovoljava uslove iz

¹⁷⁴ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (pristupljeno 5. 3. 2017).

Direktive. To je bio jedini način da garancije predviđene Direktivom imaju puno dejstvo i da se postigne delotvorna i potpuna zaštita lica na koje se podaci odnose (ili njihovog prava na privatnost).¹⁷⁵

U pogledu teritorijalne primene Direktive, Sud je primetio da je *Google Spain* društvo kći kompanije *Google Inc.* na teritoriji Španije, a stoga i „pravno lice sa poslovnim nastanjenjem“, u smislu Direktive. Sud je odbio argument da se obrada podataka o ličnosti od strane Google pretrage nije odvijala u okviru aktivnosti tog pravnog lica sa poslovnim nastanjenjem u Španiji. Sud je utvrdio da je, kada se obrada podataka o ličnosti vršila za potrebe pretraživača preduzeća koje je, iako je imalo sedište u trećoj zemlji, imalo pravno lice sa poslovnim nastanjenjem u državi članici, obrada podataka vršena „u kontekstu aktivnosti tog pravnog lica sa poslovnim nastanjenjem“, u smislu Direktive, ako je ono u toj državi članici imalo za cilj da promoviše i prodaje oglasni prostor na pretraživaču, a koji je služio za naplatu usluge koju je nudio pretraživač.

Što se tiče mere u kojoj je operator pretraživača odgovoran, Sud je utvrdio da je operator, u određenim okolnostima, bio obavezan da izbriše linkove ka internet stranicama koje su objavljivale treće strane, koji su sadržali podatke o nekom licu, sa liste rezultata pretrage koja se pojavljivala nakon pretrage izvršene po prezimenu tog lica. Sud je jasno rekao da je takva obaveza mogla postojati i pod pretpostavkom da to prezime ili te informacije nisu prethodno ili simultano izbrisani sa tih internet stranica i to, u zavisnosti od slučaja, čak i kada je njihovo objavljivanje na tim stranicama samo po sebi bilo zakonito.

Sud je u ovom kontekstu istakao da je obrada podataka o ličnosti od strane takvog operatora omogućavala bilo kom korisniku interneta da, u slučaju pretrage imena fizičkog lica, uz listu rezultata pretrage dobije i strukturirani prikaz podataka koji se odnose na to lice a koji

¹⁷⁵ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (pristupljeno 5. 3. 2017).

se mogu pronaći na internetu. Osim toga, Sud je primetio da su se te informacije potencijalno ticale mnogobrojnih aspekata privatnog života tog lica a da bez navedenog pretraživača nije bilo moguće ili jeste bilo moguće, ali vrlo teško, utvrditi međupovezanost tih informacija. Korisnici interneta su na taj način mogli da utvrde manje ili više detaljan profil lica koje je bilo predmet pretrage. Štaviše, efekat mešanja u vršenje prava tog lica bio je naglašen usled važne uloge koju internet i pretraživači imaju u modernom društvu, koji informacije sadržane u listama rezultata pretrage čine sveprisutnim. Imajući u vidu težinu koju takvo mešanje u vršenje prava može imati, prema mišljenju Suda, ono se ne može opravdati samo ekonomskim interesom operatora pretraživača u obradi podataka.

Međutim, u meri u kojoj je brisanje linkova sa liste rezultata moglo, s obzirom na informacije o kojima je reč, imati posledice na zakonit interes korisnika interneta koji su potencijalno bili zainteresovani za pristup predmetnim informacijama, Sud je konstatovao da je bilo potrebno pronaći pravednu ravnotežu između tog interesa i osnovnih prava lica na koga se podaci odnose, prava na privatnost i prava na zaštitu podataka o ličnosti. Sud je u tom smislu primetio da bi, iako prava lica na koja se podaci odnose imaju prednost nad interesom korisnika interneta, ta ravnoteža u određenim slučajevima mogla da zavisi od prirode predmetne informacije i njene osetljivosti u odnosu na privatnost lica na koje se podaci odnose, kao i u odnosu na interes javnosti za tu informaciju, koji se može razlikovati u zavisnosti od uloge koju to lice ima u javnom životu.¹⁷⁶

Na kraju, na pitanje omogućuje li Direktiva licu na koje se podaci odnose da zahteva brisanje linkova ka internet stranicama sa liste rezultata pretrage po osnovu toga što želi da navedene informacije u vezi sa njim budu „zaboravljene“ nakon nekog vremena, Sud je utvrdio da se, ako se na osnovu zahteva lica na koje se podaci odnose utvrdi da je uvrštavanje tih linkova na listu rezultata pretrage, u

¹⁷⁶ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (pristupljeno 5. 3. 2017).

toj tački u vremenu, suprotno Direktivi, ti linkovi i informacije moraju obrisati sa liste rezultata pretrage. Sud je napomenuo da bi čak i obrada tačnih podataka koja je u početku bila zakonita, tokom vremena, mogla postati suprotna Direktivi, ako su ti podaci, s obzirom na sve okolnosti slučaja, postali neadekvatni, nerelevantni, ili su prestali da budu relevantni, ili ako su preterani u odnosu na svrhu obrade, kao i na proteklo vreme. Sud je dodao da je, prilikom razmatranja takvog zahteva kojim se lice na koje se podaci odnose protivi obradi koju vrši operator pretraživača, trebalo preispitati da li je lice na koje se podaci odnose imalo pravo na to da se predmetne informacije više ne povezuju sa njim u listi rezultata pretrage koju je pretraživač prikazivao nakon izvršene pretrage na osnovu njegovog imena. Ako je odgovor da, onda se linkovi ka internet stranicama koje sadrže te informacije moraju izbrisati sa te liste rezultata pretrage, osim ako ne postoje posebni razlozi, kao što je uloga koju to lice ima u javnom životu, koji opravdavaju prevagu javnog interesa na pristup tim informacijama u okviru takve pretrage.

Sud je istakao da je lice na koje se podaci odnose moglo takav zahtev da uputi direktno operatoru pretraživača (rukovaocu podataka) koji je morao da valjano ispita njegovu osnovanost. Ako rukovalac podataka ne odobri taj zahtev, lice na koje se podaci odnose može se obratiti nadzornom ili sudskom organu radi izvršenja nužnih provera i nalažanja operatoru da preduzme određene mere u skladu sa tim.¹⁷⁷

Spojeni predmeti C-92/09 i C-93/09 Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen, presuda od 9. novembra 2010.¹⁷⁸

Sud je proglasio nevažećim propise Unije u delu o objavljivanju informacija o korisnicima poljoprivrednih fondova EU zbog nepoštovanja principa proporcionalnosti.

¹⁷⁷ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (pristupljeno 5. 3. 2017).

¹⁷⁸ <http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=891362> (pristupljeno 5. 3. 2017).

Uredba Saveta (EZ) br. 1290/2005 od 21. juna 2005. godine o finansiranju zajedničke poljoprivredne politike i Uredba Komisije (EZ) o sprovođenju br. 259/2008 predviđaju da države članice treba da osiguraju objavljivanje korisnika Evropskog fonda za garancije u poljoprivredi (EAGF) i Evropskog poljoprivrednog fonda za ruralni razvoj (EAFRD) jednom godišnje, kao i iznosa koje su primili iz svakog od ovih fondova. Poljoprivrednici su osporili objavljivanje ovih informacija na internet stranici nemačke Savezne kancelarije za poljoprivredu i hranu, pozivajući se na argument da propisi Unije predviđaju neopravdano mešanje u vršenje njihovog prava na poštovanje njihovog privatnog i porodičnog života i na zaštitu podataka o ličnosti, iz Članova 7. i 8. Povelje Evropske unije o osnovnim ljudskim pravima.¹⁷⁹

U predmetu, koji mu je upućen od strane Upravnog suda u Visbade-nu, Sud pravde je, pošto je istakao da se pravo na zaštitu podataka o ličnosti odnosi na fizička lica, kao prvo priznao postojanje takvog mešanja, zato što su navedeni podaci bili imena lica što ih je činilo, iako se tiču aktivnosti profesionalne prirode zainteresovane strane, podacima o ličnosti koji su objavljivanjem postali dostupni trećim licima. Istakao je da takva obrada podataka o ličnosti nije bila zasnovana na saglasnosti zainteresovanih strana i da je zbog toga bilo prikladno da se ispita da li je mešanje u vršenje prava potonjih bilo opravdano imajući u vidu uslove predviđene Članom 52. stav 1. Povelje.

S tim u vezi, Sud je prepoznao da je cilj predmetnih odredaba bio povećanje transparentnosti korišćenja sredstava Unije u okviru zajedničke poljoprivredne politike i da su zbog toga ispunjavale cilj koji se tiče opšteg interesa.

Sa druge strane, u pogledu proporcionalnosti mere, Sud je napravio razliku između odredaba koje se odnose na objavljivanje podataka u vezi sa pravnim licima, koje je validirao, i onih u vezi sa fizičkim licima.¹⁸⁰

¹⁷⁹ http://ec.europa.eu/dgs/legal_service/arrets/09c092_en.pdf (pristupljeno 5. 3. 2017).

¹⁸⁰ Ibid.

U slučaju potonjih, pošto je podsetio da se ograničenja prava na zaštitu podataka o ličnosti moraju primeniti samo u onoj meri u kojoj je to neophodno i da se ne može automatski dati prioritet cilju transparentnosti u odnosu na ovo pravo, Sud je utvrdio da EK i Savet nisu predložili da su pokušavali da naprave odgovarajuću ravnotežu između različitih interesa pre donošenja spornih propisa. Imajući u vidu da je bilo moguće zamisliti alternativne mere, Sud je stavio naglasak na činjenicu da je na institucijama provera da li je bilo moguće ograničiti objavljivanje podataka o imenu korisnika prema periodima za koje im je pomoć dodeljena, ili učestalosti ili prirodi i iznosu pomoći koja im je dodeljena, i uz njih objaviti relevantne podatke, po potrebi.

Shodno tome, Sud je relevantne odredbe Uredbe (EZ) br. 1290/2005 i Uredbe (EZ) br. 259/2008 proglasio nevažećim. To proglašenje nevažećim, koje se primenjuje samo u budućnosti, ne dozvoljava da se pokrenu bilo kakvi postupci radi osporavanja efekata objavljivanja spiskova imena korisnika pomoći fondova EAGF i EAFRD od strane državnih organa u periodu pre datuma donošenja presude.¹⁸¹

¹⁸¹ http://ec.europa.eu/dgs/legal_service/arrets/09c092_en.pdf (pristupljeno 5. 3. 2017).

2.6. EVROPSKI OMBUDSMAN

Evropski Ombudsman je dužan da osigura da građani, NVO, udruženja i privredni subjekti budu upoznati sa njihovim pravima na žalbu na nepravilan rad uprave u institucijama EU.

Ombudsman sprovodi postupak nadzora u pogledu poštovanja osnovnih prava, povreda zakonskih pravila i principa, poštovanja principa dobre uprave, upravnih nepravilnosti, zloupotrebe ovlašćenja, nepravедnosti, diskriminacije, bespotrebnog odugovlačenja, nedavanja ili uskraćivanja informacija. Ne postupa po pritužbama na rad nacionalnih ili lokalnih organa vlasti, fizičkih lica ili nekog EU funkcionera ili kadra lično. Njegove odluke nisu pravno obavezujuće ali je procenat postupanja po njima konzistentno visok.¹⁸²

Predmet pritužbi su najčešće zakasnele isplate, ugovorni sporovi, dodela ugovora i grantova, otvorenost i pristup dokumentima, proceduralne greške i bespotrebna odlaganja, konkursi i izbor kandidata, povrede osnovnih prava, preterana birokratija i stvari koje se tiču ustava i politike. Podnosilac pritužbe može biti oštećeno fizičko ili pravno lice, Ombudsman, kadrovi iz uprave EU ili čak anonimno lice.

Žalbe koje podnose zaposleni u EU institucijama zasnovane su na Članu 90. stav 2. Uredbe o kadrovima. One najčešće sadrže navode o neopravdanom otkazu, potraživanjima na ime socijalnog osiguranja za člana porodice ili ostalim potraživanjima u vezi sa radnim odnosom. Lice ima pravo na žalbu u roku od dve godine od dana kada je postalo svesno navodne povrede njegovih prava. On ili ona ne može da podnese žalbu u predmetima koji su već pred sudom. Žalbe uzbunjivača treba da budu poverljive.

Od trenutka prijema žalbe navodi se šalju predmetnoj ustanovi. Ustanova mora da se izjasni o navodima, dostavi informacije

¹⁸²

<https://www.ombudsman.europa.eu/en/press/introduction.faces> (pristupljeno 5. 3. 2017).

i omogućiti pristup svim predmetnim zbirkama podataka. Ombudsman može da obavi razgovor sa funkcionerima i zaposlenima.

Postoje dva moguća ishoda. Ombudsman često može samo da obavesti neku instituciju o žalbi da bi problem bio rešen. Ombudsman će pokušati da nađe sporazumno rešenje. Ukoliko se ne postigne sporazum, Ombudsman daje preporuku predmetnoj instituciji. U slučaju da institucija ne prihvati preporuke, Ombudsman upućuje poseban izveštaj Evropskom parlamentu.¹⁸³

Ombudsman prepoznaje važnu ulogu koju sredstva javnog informisanja imaju u informisanju javnog mnjenja, podsticanju razmene mišljenja i povećanju vidljivosti njenih usluga u svim zemljama članicama EU. Proaktivna medijska politika predstavlja centralni deo njenih aktivnosti i njenih napora da promoviše poštovanje prava koja proističu iz prava EU i da se poboljša kvalitet uprave.

Medijska politika Ombudsmanke zasniva se na dvostrukom pristupu: sa jedne strane, ona nastoji da informiše širu evropsku javnost o svom radu preko opštih sredstava javnog informisanja (npr. TV, novine, radio). Sa druge strane, njene aktivnosti su usmerene na određene grupe potencijalnih podnosilaca žalbi putem specijalizovanih sredstava javnog informisanja (npr. ekonomski ili potrošački časopisi, interni bilteni udruženja, NVO i interesne grupe).

Ombudsmanka ima za cilj da njen rad bude transparentan i da u najvećoj mogućoj meri bude dostupna novinarima kako bi se javnosti omogućilo da prati njen rad. Ona sredstvima javnog informisanja pruža informacije o tome da su pokrenuti postupci nadzora, da su institucije prihvatile sporazumno rešavanje spora, o važnim nacrtima preporuka koje su upućene institucijama i odlukama o završetku postupka nadzora. Ombudsmanka takođe obaveštava sredstva javnog informisanja o svom Godišnjem izveštaju, najnovijim statističkim podacima, doprinosima javnim raspravama i inicijativama, i ostalim

¹⁸³

<https://www.ombudsman.europa.eu/en/press/introduction.faces> (pristupljeno 5. 3. 2017).

temama koje su relevantne za javnost a tiču se Ombudsmankinog rada. Iako je cilj Ombudsmanke da njen rad bude što transparentniji, ona poštuje legitimne zahteve podnosilaca žalbi koji su odlučili da se njihovi slučajevi obrađuju kao poverljivi.¹⁸⁴

Predmeti

Na primer, Ombudsmanka je pokrenula strateški ispitni postupak po pitanju kašnjenja EK u postupanju po preko 200 predloga za ispitivanje hemikalija da se odredi njihova potencijalna štetnost po ljudsko reproduktivno zdravlje; da li je lečenje osoba sa invaliditetom u okviru šeme zajedničkog zdravstvenog osiguranja (JSIS) [Joint Sickness Insurance Scheme] u saglasnosti sa UN Konvencijom; obelodanjivanja dokumenata u vezi sa trijalogom i transparentnošću trijaloga uopšte od strane Evropskog parlamenta, Saveta i Evropske komisije; i o ažurnosti plaćanja EK.

U predmetu br. 2004/2013/PMC¹⁸⁵ o odbijanju odobrenja pristupa dokumentima koji se odnose na nadzor nad internetom od strane britanskih obaveštajnih službi Ombudsmanka je odlučila:

- (i) Komisija Povereniku treba da odobri pristup pismu britanskog ministra spoljnih poslova od 3. jula 2013.
- (ii) Komisija treba da odobri pristup svim ostalim dokumentima koje je tražio podnosilac žalbe koji se tiču masovnog nadzora nad internetom od strane državnih agencija UK, ili da propisno obrazloži zašto, po njenom mišljenju, zahtev za njihovo otkrivanje mora biti odbijen.

Komisija je postupila po preporuci br. (i), ali je odbila da obelodani druge dokumente oslanjajući se na svoj stav da nije postojao

¹⁸⁴ <https://www.ombudsman.europa.eu/en/press/introduction.faces> (pristupljeno 5. 3. 2017).

¹⁸⁵ Odluka u predmetu 2004/2013/PMC o postupanju Evropske komisije po zahtevima za pristup dokumentima koji se odnose na nadzor nad internetom od strane obaveštajnih službi UK, Odluka od 5. novembra 2015. i Preporuka od 2. oktobra 2014.

pretežniji javni interes za njihovo otkrivanje, dok bi objavljivanje pre završetka istrage predstavljalo rizik od spoljnih pritisaka.

Kritička primedba je bila da: *Komisija nije predočila valjane razloge za odbijanje zahteva za pristup predstavkama građana i njenim pismima državnim organima UK. To predstavlja nepravilan rad uprave, i to naročito težak nepravilan rad imajući u vidu značaj predmeta o kome je reč.*

Faktori koje je Ombudsmanka razmatrala prilikom određivanja da li postoji pretežniji javni interes za obelodanjivanje dokumenata bili su:

- predmet dokumenata se odnosi na osnovno pravo građana EU – pravo na zaštitu podataka,
- iz pisama britanskog ministra spoljnih poslova evidentno je da se ova situacija ne tiče državnih organa UK,
- pismo britanskog ministra spoljnih poslova datira iz jula 2013. godine, EK nije preduzela nikakve konkretne istražne radnje do odluke Ombudsmanke 2015. godine.

Ombudsmanka je takođe usvojila tri odluke o primeni metoda procene dodatnih sposobnosti kandidata [Talent Screener] u postupku izbora od strane Evropskog zavoda za izbor kadrova (EPSO). Prema navodima, EPSO nije definisao jasne uslove za učešće u postupku izbora kandidata. Podnosioci predstavke su tvrdili da EPSO treba, u budućim konkursima, da kandidate bolje informiše o tome kako će se ovaj metod primenjivati.

U ovom slučaju, podnosilac predstavke je eliminisan nakon prvog kruga primene metoda procene dodatnih sposobnosti, jer nije dobio prolaznu ocenu. Ta prolazna ocena bila je definisana na osnovu samoprocene svih kandidata, a da Komisija za izbor nije potvrdila tačnost njegovog odgovora. Službenički sud je utvrdio da bi, u odnosu na konkurs u kome je primenjen metod procene dodatnih sposobnosti, moglo da se desi da kandidati sa superiornim kvalifikacijama budu eliminisani iz postupka izbora kandidata, kao rezultat

toga što su manje kvalifikovani kandidati: (i) tumačili pitanja metodom procene dodatnih sposobnosti na način koji je preterano povoljan u poređenju sa njihovim kvalifikacijama i stručnim iskustvom; (ii) pogrešno razumeli pitanja; i/ili (iii) neprecizno procenili svoje akademske kvalifikacije ili stručno iskustvo.¹⁸⁶

U sva tri slučaja Ombudsmanka je predložila sporazumno rešenje: „EPSO bi trebalo da razmotri da zatraži od Komisije za izbor kandidata da sprovede detaljnu analizu pisanih odgovora podnosioca predstavke, dodeli poene za svako pitanje gde je podnosilac predstavke dao odgovor „da“ i da mu, ako je ukupna ocena iznad određenog odgovarajućeg broja poena, omogućiti učešće u sledećem krugu postupka izbora kandidata“.

EPSO je prihvatio Ombudsmanov predlog sporazumnog rešavanja i naveo da će zatražiti od Komisije za izbor kandidata da proceni predmet podnosioca predstavke. Podnosilac predstavke je bio zadovoljan ishodom i zahvalio se Ombudsmanki.

¹⁸⁶

<https://www.ombudsman.europa.eu/en/press/introduction.faces> (pristupljeno 5. 3. 2017).

2.7. EVROPOL

Evropol je agencija za sprovođenje zakona Evropske Unije. Sa sedištem u Hagu, Holandija, ona pomaže 28 država članica EU u njihovoj borbi protiv ozbiljnog međunarodnog kriminala i terorizma. On takođe sarađuje sa mnogim partnerskim državama van EU i sa međunarodnim organizacijama.¹⁸⁷

Široko rasprostranjena mreža kriminala i terorizma predstavlja značajnu pretnju unutrašnjoj bezbednosti EU. Terorizam, visokotehnoški kriminal i šverc ljudi, da imenujemo samo neke, predstavljaju ozbiljnu pretnju bezbednosti i životu ljudi u EU.

Ali nove opasnosti takođe rastu, kao što su on-lajn radikalizacija i trgovina ljudima. Mreže iza kriminala u svakoj od ovih oblasti brzo grabe nove mogućnosti, i one su otporne u suočavanju sa tradicionalnim merama sprovođenja zakona.

Evropol podržava organe koji sprovode zakon širom EU u vezi aktivnosti borbe protiv kriminala, u svim oblastima za koje ima mandat (kako je detaljno izneto u Odluci Saveta Evrope¹⁸⁸, kojom se osniva Evropska policijska kancelarija).

Operativne aktivnosti

Ove aktivnosti se fokusiraju na:

- nezakonite droge/lekove;
- trgovinu ljudima;
- omogućene ilegalne migracije;
- visokotehnoški kriminal;
- zločin protiv prava intelektualne svojine;
- švercovanje cigareta;

¹⁸⁷ <https://www.europol.europa.eu/about-europol> (pristupljeno 14. 3. 2017).

¹⁸⁸ Odluka Saveta od 6. aprila 2009. godine kojom se osniva Evropska policijska kancelarija (European Police Office – Europol), OJ L 121/37.

- krivotvorenje evra;
- prevara u vezi PDV-a;
- pranje novca i poreklo imovine;
- mobilne grupe organizovanog kriminala;
- terorizam.

Upravljanje i kontrola

Evropol je na nivou EU odgovoran Savetu ministara za pravosuđe i unutrašnje poslove.

Savet je odgovoran za glavnu kontrolu i usmeravanje Evropola. On postavlja direktora i zamenike direktora, i zajedno sa Evropskim parlamentom odobrava budžet Evropola (koji predstavlja deo opšteg budžeta EU). Savet takođe može usvojiti, zajedno sa Evropskim parlamentom, propise vezane za rad Evropola. Svake godine Savet Evropskom parlamentu prosleđuje Specijalni izveštaj o radu Evropola.¹⁸⁹

Zaštita podataka

U oblasti sprovođenja zakona, najviši standardi zaštite podataka i bezbednosti su od najvećeg značaja.

Od momenta osnivanja Evropola bilo je jasno da će se morati stvoriti skup prilagođenih pravila, koja uzimaju u obzir i operativne potrebe Evropola i prava pojedinca na efikasnu zaštitu podataka.

Sakupljanje i obrada podataka su u srcu rada Evropola, i on skladišti velike količine ličnih podataka. Različite jedinice Evropola, države članice EU i čak i treće strane prosleđuju ih jedna drugoj radi analize. Za neke, ovakva slika može davati razloga za zabrinutost.

¹⁸⁹ <https://www.europol.europa.eu/about-europol> (pristupljeno 14. 3. 2017).

Neprevaziđeni načini na koje Evropol i druge organizacije mogu sakupiti i analizirati podatke ovih dana donose sa sobom obavezu poštovanja svačijeg prava da njihovi lični podaci budu propisno zaštićeni. Da bi delovao u skladu sa ovom obavezom, Evropol mora minimizovati opasnost zloupotrebe i rizik curenja podataka, bilo namernog ili nehotičnog.¹⁹⁰

Evropol je ponosan što poseduje jedan od **najčvršćih okvira zaštite podataka u svetu sprovođenja zakona**. To je prednost, čak iako ona nameće značajne odgovornosti, uključujući dužnost da se u svakodnevnim operacijama obezbedi primena tog okvira.

Postoje dva tela koja rade u okviru ili sa Evropolom, radi obezbeđenja sprovođenja i praćenja postupaka za zaštitu podataka: Kancelarija za zaštitu podataka (Data Protection Office – DPO) i Zajedničko nadzorno telo (Joint Supervisory Body – JSB).

Kancelarija za zaštitu podataka (KZP) je sastavni deo Evropola i početna tačka kontakta za sva pitanja zaštite podataka. Jedinicom rukovodi Službenik za zaštitu podataka, koga postavlja Upravni odbor na osnovu predloga direktora. Kancelarija za zaštitu podataka, koja postupuje nezavisno, blisko sarađuje sa osobljem Evropola, nudeći savet i usmerenje u skladu sa najboljom praksom u obradi ličnih podataka.

Pravila zaštite podataka su merodavna za sve oblike razmene ličnih podataka između Evropola i država članica.

Kancelarija za zaštitu podataka ima pristup svim podacima obrađenim od strane Evropola i svim prostorijama Evropola. Njena glavna aktivnost je obezbeđivanje zakonske usklađenosti sa Odlukom Saveta, koja definiše mandat Evropola u vezi obrade ličnih podataka, uključujući podatke osoblja Evropola.

Pojedinac može dobiti informacije o tome da li je bilo koji od njegovih ličnih podataka bio obrađen u sistemima Evropola i da mu/

¹⁹⁰ <https://www.europol.europa.eu/about-europol> (pristupljeno 14. 3. 2017).

njoj takvi podaci budu saopšteni, ili provereni. U tu svrhu, pojedinac može podneti zahtev Evropolu putem nadležnog organa za zaštitu podataka neke države članice. U Evropolu, Kancelarija za zaštitu podataka preduzima neophodne provere.

Zajedničko nadzorno telo

Dok je Kancelarija za zaštitu podataka, iako nezavisna u obavljanju njenih zadataka, sastavni deo organizacije, Zajedničko nadzorno telo (Joint Supervisory Body – JSB) sprovodi spoljne provere.

Zajedničko nadzorno telo se sastoji od dva predstavnika iz svakog od nacionalnih organa za zaštitu podataka u EU. Predstavnike postavljaju njihove države članice na period od pet godina. Svaka delegacija ima pravo na jedan glas u Zajedničkom nadzornom telu.

Ovi stručnjaci poseduju značajno iskustvo u obradi podataka u okruženju sprovođenja zakona. Oni često pregledaju aktivnosti Evropola iz perspektive zaštite podataka. U tu svrhu, Zajedničko nadzorno telo poseduje ovlašćenje za inspekciju svih dosijea Evropola u bilo koje vreme. Ono se poziva na to pravo barem jednom godišnje, putem inspekcijske posete prostorijama Evropola, u bliskoj saradnji sa Kancelarijom za zaštitu podataka. Ta inspekcija obuhvata sve Evropolove operacije obrade, na osnovu kojih se isporučuje opsežan i detaljan izveštaj koji uključuje nalaze i preporuke. To telo takođe sprovodi *ad hoc* inspekcije po potrebi.¹⁹¹

Pored gorenavedenih provera koje sprovode Kancelarija za zaštitu podataka i Zajedničko nadzorno telo, svaka država članica ima sopstveno nacionalno nadzorno telo. U skladu sa njenim nacionalnim zakonom, svaka država članica proverava prenos ličnih podataka do i od Evropola. Članovi svakog od ovih nacionalnih nadzornih tela takođe imaju pristup dokumentima i prostorijama njihovih Oficira za vezu¹⁹² pri Evropolu.

¹⁹¹ <https://www.europol.europa.eu/about-europol> (pristupljeno 14. 3. 2017).

¹⁹² <https://www.europol.europa.eu/partners-agreements> (pristupljeno 5. 3. 2017).

Ciljevi

Strategija usmerava Evropol u praktičnom sprovođenju njegovih glavnih ciljeva i vizije, i u isporuci jedinstvenog skupa operativnih usluga za EU.

Evropolova tri glavna cilja su da postane informaciono kriminalističko čvorište za EU, koje će obezbediti sposobnosti za deljenje informacija organima za sprovođenje zakona u državama članicama; da raste kao centralno informaciono kriminalističko čvorište za EU; da obezbedi najefikasniju operativnu podršku i ekspertizu u istragama u državama članicama razvijanjem i korišćenjem sveobuhvatnog portfelja službi i da postane efikasna organizacija sa efektinim aranžmanima upravljanja i pozitivnom reputacijom.¹⁹³

Centri

Skorijih godina Evropol je lansirao namenske centre koji se fokusiraju na specifične pretnje sa kojima se EU suočava:

- Evropski centar za visokotehnoški kriminal (European Cyber-crime Centre – EC3)¹⁹⁴;
- Evropski centar za švercovanje migranata (European Migrant Smuggling Centre – EMSC)¹⁹⁵;
- Evropski centar za borbu protiv terorizma (European Counter Terrorism Centre – ECTC)¹⁹⁶;

¹⁹³ <https://www.europol.europa.eu/about-europol> (pristupljeno 14. 3. 2017).

¹⁹⁴ <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (pristupljeno 27. 2. 2017).

¹⁹⁵ <https://www.europol.europa.eu/about-europol/european-migrant-smuggling-centre-emsc> (pristupljeno 27. 2. 2017).

¹⁹⁶ <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc> (pristupljeno 27. 2. 2017).

- Koalicija za koordinaciju borbe protiv krivičnih dela protiv intelektualne svojine (Intellectual Property Crime Coordination Coalition – IPC3)¹⁹⁷.

EC3 je uspostavljen 2013, EMSC, ECTC i IPC3 2016. godine. Iste godine, Jedinica za finansijsko-obaveštajne poslove¹⁹⁸, decentralizovana i posvećena kompjuterska mreža koja podržava Jedinice za finansijsko-obaveštajne poslove (Financial Intelligence Units – FIUs) u EU u njihovoj borbi protiv pranja novca i finansiranja terorizma – postala je deo operacija Evropol, potez od koga se očekuje da dalje premosti jaz finansijsko-obaveštajnih operacija i stvori veću sinergiju između svih zajednica koje upravljaju finansijsko-obaveštajnim poslovima u državama članicama.

2016. godine Evropska mreža timova za aktivno traganje za beguncima (European Network of Fugitive Active Search Teams – ENFAST) lansirala je, a Evropol omogućio hosting veb sajta, koji navodi najtraženije kriminalce koji su optuženi za ili su osuđeni za ozbiljne zločine u Evropi, kao što su ubistvo, seksualna eksploatacija dece, oružana pljačka i terorizam. Javnost može pružiti pomoć putem samog veb sajta, anonimno ako se tako želi.

Prvog maja 2017. godine stupio je na snagu novi propis Evropol¹⁹⁹, koji omogućava Evropolu da pojača svoje napore u borbi protiv terorizma, visokotehnološkog kriminala i drugih ozbiljnih i organizovanih oblika kriminala. Nova ovlašćenja Evropol biće praćena povećanim zaštitnim merama za zaštitu podataka, demokratsku kontrolu i detaljno praćenje Parlamenta.

¹⁹⁷ <https://www.europol.europa.eu/about-europol/intellectual-property-crime-coordinated-coalition-ipc3> (pristupljeno 27. 2. 2017).

¹⁹⁸ <https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net> (pristupljeno 27. 2. 2017).

¹⁹⁹ <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0121> (pristupljeno 27. 2. 2017).

2.8. "EUROJUST"

Da bi pojačao borbu protiv ozbiljnog organizovanog kriminala, Savet Evrope, u svom Zaključku 46, ugovorio je da se uspostavi jedinica ("Eurojust"), sastavljena od 28 nacionalnih članova, odnosno tužilaca, sudija, sudija za prekršaje, ili činovnika policije ekvivalentne nadležnosti, delegiranih iz svake države članice u skladu sa njihovim odgovarajućim pravnim sistemima. Nacionalni članovi podležu nacionalnom zakonodavstvu država članica koje ih postavljaju u vezi svog statusa, što takođe određuje mandat, kao i prirodu i opseg njima prenetih sudskih nadležnosti.²⁰⁰

Napadima od 11. septembra u SAD, fokus borbe protiv terorizma pomerio se sa regionalne /nacionalne sfere na njen najširi međunarodni kontekst i poslužio kao katalizator za formalizaciju, putem Odluke Saveta 2002/187/JHA, osnivanja "Eurojust"-a kao jedinice za pravosudnu koordinaciju. U 2002. godini Odluka o "Eurojust"-u objavljena je 28. februara, budžet je odobren u maju, a Poslovnik je usaglašen u junu. 29. aprila 2003. godine "Eurojust" je premestio svoje sedište u Hag.

U julu 2008. Savet Evrope je odobrio novu Odluku Saveta o jačanju "Eurojust"-a, koja je ratifikovana decembra 2008. i objavljena 4. juna 2009. godine. Svrha nove Odluke je da unapredi operativne sposobnosti "Eurojust"-a, poveća razmenu informacija između zainteresovanih strana, olakša i ojača saradnju između nacionalnih organa i "Eurojust"-a, i da ojača i uspostavi odnose sa partnerima i trećim državama.

Najnovije poglavlje u razvoju "Eurojust"-a sadržano je u Međudržavnom ugovoru iz Lisabona (Lisbon Treaty), naime u Poglavlju 4, Članovima 85. i 86. Član 85. spominje "Eurojust" i definiše njegovu misiju, *da podrži i ojača koordinaciju i saradnju između nacionalnih istražnih i organa tužilaštva u vezi ozbiljnih zločina koji pogađaju dve*

²⁰⁰

<http://www.eurojust.europa.eu/about/background/Pages/History.aspx> (pristupljeno 15. 3. 2017).

ili više država članica[...]. Član 86. navodi da, radi borbe protiv zločina koji utiču na finansijske interese Unije, Savet, putem propisa usvojenih u skladu sa specijalnim zakonodavnim postupkom, može osnovati od 'Eurojust'-a Evropsko javno tužilaštvo.

Odluka Saveta 2002/187/JHA od 28. februara 2002. godine, koja uspostavlja "Eurojust" u cilju jačanja borbe protiv ozbiljnog kriminala²⁰¹, kako je dopunjeno Odlukom Saveta 2003/659/JHA²⁰² i Odlukom Saveta 2009/426/JHA od 16. decembra 2008, o jačanju "Eurojust"-a²⁰³ obezbeđuje pravnu osnovu za funkcionisanje "Eurojust"-a.

Nadležnosti

"Eurojust" stimuliše i poboljšava koordinaciju istraga i krivičnog gonjenja između nadležnih organa u državama članicama i poboljšava saradnju između nadležnih organa istih, naročito olakšavajući izvršenje međunarodne uzajamne sudske pomoći i u praktičnom sprovođenju zahteva za ekstradiciju. "Eurojust" na svaki mogući način podržava nadležne organe država članica da njihove istrage i krivična gonjenja budu efikasniji kada se bave prekograničnim kriminalom.²⁰⁴

Na zahtev neke države članice, "Eurojust" može pomoći u istragama i krivičnim gonjenjima koji se tiču te naročite države članice i neke

²⁰¹ Odluka Saveta 2002/187/JHA, od 28. februara 2002. godine, kojom se uspostavlja "Eurojust" u cilju jačanja borbe protiv ozbiljnog kriminala, OJ L 063, 06/03/2002, str. 0001–0013.

²⁰² Odluka Saveta 2003/659/JHA, od 18. juna 2003. godine, koja dopunjuje Odluku 2002/187/JHA kojom se uspostavlja "Eurojust" u cilju jačanja borbe protiv ozbiljnog kriminala, OJ L 245, 29/09/2003, str. 0044–0046.

²⁰³ Odluka Saveta 2009/426/JHA, od 16. decembra 2008. godine, o jačanju "Eurojust"-a i kojom se menja i dopunjuje Odluka 2002/187/JHA kojom se uspostavlja "Eurojust" u cilju jačanja borbe protiv ozbiljnog kriminala.

²⁰⁴ <http://www.eurojust.europa.eu/about/background/Pages/eurojust-core-business.aspx> (pristupljeno 13. 3. 2017).

države koja nije članica, ako je zaključen ugovor o saradnji ili je prikazan suštinski interes u obezbeđivanju takve pomoći.

Nadležnost “Eurojust”-a obuhvata iste vrste zločina i krivičnih dela za koje je nadležan Evropol, kao što su terorizam, trgovina drogom, trgovina ljudima, krivotvorenje, pranje novca, kompjuterski kriminal, krivična dela protiv imovine ili javnih dobara, uključujući prevaru i korupciju, krivična dela koja pogađaju finansijske interese EU, zločin protiv životne sredine i učešće u nekoj kriminalnoj organizaciji. Za druge vrste krivičnih dela “Eurojust” može pomagati u istragama i krivičnim gonjenjima na zahtev neke države članice.

“Eurojust” može tražiti od nadležnih organa uključenih država članica da:

- istraže ili krivično gone specifična dela;
- se koordinišu međusobno;
- prihvate da je jedna zemlja bolje pozicionirana za krivično gonjenje nego druga;
- uspostave Zajednički istražni tim; ili
- dostave “Eurojust”-u informacije neophodne za izvršenje njegovih zadataka.

Pored toga, “Eurojust”:

- obezbeđuje da nadležni organi informišu jedni druge o istragama i krivičnim gonjenjima o kojima su oni informisani;
- pomaže nadležnim organima u obezbeđivanju najbolje moguće koordinacije istraga i krivičnih gonjenja;
- pruža pomoć radi poboljšanja saradnje između nadležnih nacionalnih organa, na osnovu analize Evropola, olakšavanjem uzajamne pravne pomoći i izvršavanjem instrumenata uzajamnog priznavanja, kao što je Evropski nalog za hapšenje;
- sarađuje i konsultuje se sa Evropskom pravosudnom mrežom (European Judicial Network – EJNI), i koristi i doprinosi poboljšanju njene dokumentarne baze podataka;
- može, u skladu sa njegovim ciljevima, pokušati da poboljša saradnju i koordinaciju između nadležnih organa, i da prosledi

zahteve za pravosudnu pomoć kada su oni: (i) načinjeni od strane nadležnog organa neke države članice, (ii) tiču se neke istrage ili krivičnog gonjenja koje sprovodi taj nadležni organ u nekom specifičnom slučaju, i (iii) za njih je neophodna njegova intervencija u cilju koordinisane aktivnosti;

- može pomagati Evropolu, naročito mišljenjima zasnovanim na analizama koje su sprovedene od strane Evropola; i
- može dostaviti logističku podršku, to jest pomoć u prevođenju, tumačenju i organizaciji koordinacionih sastanaka;
- u neoperativnim strateškim pitanjima može blisko sarađivati sa institucijama EU i država članica, kao što su Evropski parlament, nacionalni parlamenti, Savet i Komisija.

Radi izvršenja njegovih zadataka “Eurojust” održava privilegovane odnose sa Evropskom pravosudnom mrežom, Evropolom, Evropskom kancelarijom za borbu protiv prevare (European Anti-Fraud Office – OLAF) i Prekršajnim sudijama za vezu. Moguće je takođe, putem Saveta, zaključiti ugovore o saradnji sa državama koje nisu članice i međunarodnim organizacijama ili telima za razmenu informacija, ili za premeštaj činovnika.

“Eurojust” je uspostavio kontakt tačke u 23 države koje nisu članice: Albanija, Argentina, Bosna i Hercegovina, Kanada, Egipat, Bivša Jugoslovenska Republika Makedonija, Island, Izrael, Japan, Koreja, Lihtenštajn, Moldavija, Mongolija, Crna Gora, Norveška, Ruska Federacija, Srbija, Singapur, Švajcarska, Tajland, Turska, Ukrajina i SAD. Koreja se poslednja pridružila.²⁰⁵

²⁰⁵

<http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx> (pristupljeno 23. 2. 2017).

Iz razloga što su zločini koji prete građanima Evrope često globalni po svojoj prirodi, "Eurojust" je sarađivao sa različitim partnerima²⁰⁶ kako bi se pomoglo u odgovoru na ovu pretnju. Pregovarao je za ugovore o saradnji za razmenu pravosudnih informacija i ličnih podataka van EU. Ugovori su zaključeni sa Norveškom, Islandom, SAD, Švajcarskom i Bivšom Jugoslovenskom Republikom Makedonijom. Tužioci za vezu iz Norveške, Švajcarske i SAD smešteni su u "Eurojust"-u . U dodatku ugovorima o saradnji, "Eurojust" održava mrežu kontakt tačaka van EU i potpisao je Protokole o saglasnosti sa telima kao što su Kancelarija Ujedinjenih nacija za borbu protiv droge i kriminala i "IberRed".

"Eurojust" igra značajnu ulogu u koordinisanju istraga i postupaka krivičnog gonjenja u vezi zaštite finansijskih interesa EU. OLAF (Evropska kancelarija za borbu protiv prevare – European Anti-Fraud Office) sprovodi upravne istrage zločina koji utiču na finansijske interese EU i prosleđuje bitne informacije "Eurojust"-u kad god se čini da neki slučaj neposredno uključuje pravosudnu saradnju između nadležnih nacionalnih organa dve ili više država članica, ili gde se taj slučaj tiče neke države članice i EU.

"Eurojust"-ov i CEPOL-ov Protokol o saglasnosti stupio je na snagu u cilju definisanja, ohrabrivanja i poboljšanja obuke za policiju i tužioce u borbi protiv ozbiljnog kriminala, naročito organizovanog kriminala. Unutar granica njegovog pravnog okvira, "Eurojust" će informisati CEPOL o njegovim prioritetima i aktivnostima, radi omogućavanja CEPOL-u da u skladu sa tim planira svoje aktivnosti obuke. EMCDDA (Evropski centar za praćenje droga i zavisnosti od droge – European Monitoring Centre for Drugs and Drug Addiction) Protokol se fokusira na pitanja vezana za drogu, bitna za sudsku saradnju – uključujući nabavku droge, smanjenje nabavke droge i zakonodavstvo.²⁰⁷

²⁰⁶ <http://www.eurojust.europa.eu/about/Partners/Pages/eu-institutions-agencies-and-bodies.aspx> (pristupljeno 27. 2. 2017).

²⁰⁷ Ibid.

Zajednički istražni timovi

Zajednički istražni tim (Joint Investigation Team – JIT) je tim koji se sastoji od sudija, tužilaca i organa za sprovođenje zakona, osnovan za neki tačno određen period i za specifičnu svrhu putem pisanog sporazuma između uključenih država, radi sprovođenja krivične istrage u jednoj ili više uključenih država. Mogućnost uspostavljanja JIT-ova između država članica predviđena je u Članu 13. Konvencije o uzajamnoj pravnoj pomoći iz 2000. godine. U svetlu sporog napredovanja ka njenoj ratifikaciji, Savet je usvojio 13. juna 2002. Okvirnu odluku o JIT-ovima, koju su države članice trebalo da praktično sprovedu do 1. januara 2003. godine.

Radi promovisanja uspostavljanja takvih timova, Haški program (novembar 2004. godine) pozvao je na postavljenje nacionalnih stručnjaka u zajedničke istražne timove od strane svake države članice, u cilju ohrabrivanja korišćenja JIT-ova i razmene najbolje prakse. U julu 2005. godine, Član 36. Odbora (CATS) izneo je saglasnost da treba osnovati neformalnu Mrežu stručnjaka za JIT-ove (videti Dokument Saveta 11037/05²⁰⁸).

Zajedničko nadzorno telo

Zajedničko nadzorno telo (ZNT) je nezavisni nadzorni organ, osnovan Članom 23. Odluke “Eurojust”-a, koji zajednički nadzire aktivnosti “Eurojust”-a koje uključuju obradu ličnih podataka i osigurava da se obrade odvijaju u skladu sa Odlukom “Eurojust”-a. Članovi Zajedničkog nadzornog tela su sudije ili lica sa podjednakim nivoom nezavisnosti (u praksi, poverenici za zaštitu podataka) i stoga poseduju prilično stručno znanje u poljima zaštite podataka i pravosudne saradnje.

²⁰⁸ <http://www.eurojust.europa.eu/doclibrary/JITs/JITs%20framework/Council%20Document%20establishing%20the%20JITs%20Network/JITs-Council-document-11037-05-EN.pdf> (pristupljeno 27. 2. 2017).

Da bi ispunilo ove zadatke, Zajedničko nadzorno telo ima potpuni pristup svim dosijeima gde se takvi lični podaci obrađuju. “Eurojust” će dostaviti Zajedničkom nadzornom telu sve informacije iz takvih dosijea koje Zajedničko nadzorno telo zahteva i pomagaće tom telu u njegovim zadacima na svaki drugi način. Usklađenost sa pravilima je kamen temeljac aktivnosti Zajedničkog nadzornog tela. Stoga, Zajedničko nadzorno telo sprovodi redovne inspekcije na licu mesta i stalno nadziranje i praćenje svih preporuka izdatih u izveštajima inspekcije. Navedeno telo takođe razmatra sa Službenikom za zaštitu podataka “Eurojust”-a (Kancelarija za zaštitu podataka) rezultate godišnjeg pregleda nivoa usklađenosti i beleži bilo koju materiju koja zahteva njegovu pažnju, radi obezbeđenja da se dobar pregled nivoa usklađenosti unutar organizacije održava u sva vremena.²⁰⁹

Zajedničko nadzorno telo je instanca obeštećenja za “Eurojust”-ovu Kancelariju za zaštitu podataka u slučajevima gde je otkrivena nesaglasnost, koju Kolegijum “Eurojust”-a nije rešio unutar nekog razumnog vremena.

Zajedničko nadzorno telo ispituje žalbe koje su mu podnete u skladu sa Članovima 19(8). i 20(2). Odluke “Eurojust”-a i sprovodi kontrole. Ako Zajedničko nadzorno telo razmatra da neka odluka doneta od strane “Eurojust”-a ili obrada podataka s njegove strane nije u skladu sa Odlukom “Eurojust”-a, to pitanje će biti upućeno “Eurojust”-u, koji će prihvatiti odluku Zajedničkog nadzornog tela. Odluke Zajedničkog nadzornog tela će biti konačne i obavezujuće za “Eurojust”.

Zajedničko nadzorno telo takođe pruža svoje obavezujuće mišljenje u vezi sa odredbama o zaštiti podataka u ugovorima ili radnim aranžmanima sa telima EU, ili ugovorima o saradnji sa trećim državama.²¹⁰

²⁰⁹ <http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/jsb/jsb/The%20Role%20of%20the%20Joint%20Supervisory%20Body%20of%20Eurojust%20%28leaflet%29/Role-of-JSB-EN.pdf> (pristupljeno 27. 2. 2017).

²¹⁰ Ibid.

Uloga Službenika za zaštitu podataka u “Eurojust”-u definisana je Članom 17. Odluke “Eurojust”-a. Službenik za zaštitu podataka je specijalno postavljen član osoblja “Eurojust”-a, kome je poveren glavni zadatak obezbeđivanja, na nezavisan način, zakonitosti i usklađenosti sa odredbama Odluke “Eurojust”-a u vezi obrade ličnih podataka i bilo kojih drugih merodavnih pravila. U izvršavanju dužnosti, na koje se upućuje u Odluci “Eurojust”-a, Službenik za zaštitu podataka postupa nezavisno.

Jedan od značajnih zadataka Službenika za zaštitu podataka je da postupa kao veza između “Eurojust”-a i Zajedničkog nadzornog tela (ZNT) radi obezbeđivanja da su članovi ZNT-a dovoljno informisani o aktivnostima “Eurojust”-a u vezi sa pitanjima zaštite podataka i praktičnog sprovođenja pravila. Na svakom sastanku, ZNT razmenjuje gledišta sa Službenikom za zaštitu podataka, koji informiše članove o svim tekućim pitanjima i o stavkama koje mogu zahtevati njihovu pažnju u budućnosti. Jaka saradnja Službenika za zaštitu podataka i Zajedničkog nadzornog tela stvara korist i u zadovoljavanju njihovih odgovornosti za obezbeđenje primene standarda za zaštitu podataka.²¹¹

U skladu sa Članom 27. Pravila o zaštiti podataka “Eurojust”-a²¹², Službenik za zaštitu podataka sprovodi godišnje preglede o usklađenosti sa Pravilima “Eurojust”-a za zaštitu podataka. Službenik za zaštitu podataka podnosi izveštaj Kolegijumu i Zajedničkom nadzornom telu o rezultatima ovih pregleda. Ova informacija se uzima u razmatranje od strane Zajedničkog nadzornog tela pri izvršavanju njegovih nadzornih zadataka, naročito njihovih inspekcija.

²¹¹ <http://www.eurojust.europa.eu/Practitioners/Data-Protection/Pages/data-protection-officer.aspx> (pristupljeno 16. 3. 2017).

²¹² Poslovnik o obradi i zaštiti ličnih podataka u “Eurojust”-u (Tekst je jednoglasno usvojen od strane Kolegijuma “Eurojust”-a tokom sastanka 21. oktobra 2004. i odobren je od strane Saveća 24. februara 2005. godine), na raspolaganju na: <http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/dataprotection/Eurojust%20Data%20Protection%20Rules/Eurojust-Dataprotection-Rules-2005-02-24-EN.pdf> (pristupljeno 27. 2. 2017).

Službenik za zaštitu podataka je interni revizor organizacije, ali nije samo to. Bilo ko kô drži neku poziciju u “Eurojust”-u može ukazati Službeniku za zaštitu podataka na neki navodni prekršaj odredbi u vezi sa obradom ličnih podataka, ili tražiti od Službenika za zaštitu podataka bilo koju vrstu saveta o pitanjima u vezi sa zaštitom podataka i obradom podataka. U slučaju navodne povrede, Službenik za zaštitu podataka sprovede istragu u bliskoj saradnji svih uključenih strana.

U slučaju neusaglašenosti, Službenik za zaštitu podataka neposredno informiše Kolegijum i Izvršnog direktora i, ako rešenje tog problema ne može da se nađe interno, Zajedničko nadzorno telo. Zajedničko nadzorno telo može ispraviti neku situaciju ili nametnuti opšte mere za poboljšanje zaštite podataka u “Eurojust”-u.

Službenik za zaštitu podataka se povezuje sa drugim organima za zaštitu podataka, kancelarijama za zaštitu podataka drugih evropskih institucija, Evropolom i Evropskim supervizorom za zaštitu podataka, razmenjujući gledišta i pomažući da se unapredi rad “Eurojust”-a. Službenik za zaštitu podataka prati sve zakonodavne inicijative vezane za zaštitu podataka koje se planiraju na nivou Evrope, radi obezbeđenja da “Eurojust” bude informisan o razvoju oblasti zaštite podataka i da može doprinositi ovim predlozima.²¹³

Zaključak

Osnovna prava utemeljena u EU razvijaju se tokom vremena i nastavljaju da evoluiraju. Pravo na zaštitu podataka je ključni deo pejzaža osnovnih prava (EU) i EU institucije igraju naročito značajnu ulogu po tom pitanju. Te institucije su čuvari ovog osnovnog prava.

Zaštita podataka se pojavljuje kao ključna oblast politike EU. Bivša Poverenica za pravosuđe, osnovna prava i građanstvo, Viviane

²¹³ <http://www.eurojust.europa.eu/Practitioners/Data-Protection/Pages/data-protection-officer.aspx> (pristupljeno 16. 3. 2017).

(Vivijen) Reding, 2011. godine naglasila je u pisanoj izjavi Evropskom parlamentu da je zaštita podataka stavka od naročitog značaja za EU. Ona je izjavila da je njeno *čvrsto uverenje da ne može biti poverenja građana u Evropu ako ne ostanemo budni u obezbeđivanju da su lični podaci zaštićeni od neovlašćene upotrebe i da građani imaju pravo da sami odluče da li da se njihovi podaci obrađuju.*

Evropski parlament se, zajedno sa Savetom EU i Evropskom komisijom, poziva da uvedu zakonodavne reforme radi garantovanja efikasnosti režima zaštite podataka. U tom smislu, ohrabruje usvajanje novog GDPR-a koji će stupiti na snagu u 2018. godini. Štaviše, Evropski sud pravde uvek je zauzimao proaktivni stav u vezi sa zaštitom podataka. Tako je on protumačio izvestan instrument usklađivanja internog tržišta (Direktiva 95/46/EC) na takav način da je podstakao zaštitu temeljnog prava unutar EU, čak i pre GDPR-a. U tom smislu, Sud je usvojio opsežno čitanje zaštitnog delokruga Direktive, koja je otišla dalje od izvršavanja privrednih aktivnosti i ograničavajućeg tumačenja oblasti izuzetih od zaštite. Štaviše, mišljenja i preporuke Radne grupe doprinose razvoju zajedničkog EU standarda sa visokim nivoom zaštite ličnih podataka. EDPS-u je takođe poveren zadatak obezbeđivanja da temeljna prava i slobode fizičkih lica i njihovo pravo na privatnost budu ispoštovani od strane EU institucija i tela. Zadatak konsultacija sa EDPS-om je značajan zato što on doprinosi zaštiti temeljnih sloboda građana Unije kada se donosi novo zakonodavstvo.

BIBLIOGRAFIJA



1. The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights, 3 September 1953.
2. Charter of Fundamental Rights of the European Union, 7 December 2000, Official Journal of the European Communities, 18 December 2000 (2000/C 364/01).
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals about the processing of personal data and on the free movement of such data, Official Journal L281, 23 November 1995, p. 31.
4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002, pp. 37–47.
5. Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), OJ L 108, 24 April 2002, pp. 21–32.
6. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13 April 2006, pp. 54–63.
7. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities

- responsible for the enforcement of consumer protection laws, OJ L 337, 18 December 2009, pp. 11–36.
8. Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, OJ L53/1.
 9. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12 January 2001, pp. 1–22.
 10. 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), OJ L 119, 4 May 2016, pp. 1–88.
 11. Rules of Procedure of the Commission, 1 January 2001, OJ L 308, 8 December 2000.
 12. Council Decision of 6 April 2009 Establishing the European Police Office (Europol), OJ L 121/37.
 13. Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view of reinforcing the fight against serious crime, OJ L 063, 6 March 2002, pp. 1–13.
 14. Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 245, 29 September 2003, pp. 44–46.
 15. Council decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime.
 16. Rules of Procedure on the Processing and Protection of Personal Data at Eurojust (Text adopted unanimously by the college of Eurojust during the meeting of 21 October 2004 and approved by the Council on 24 February 2005).

Precedentno pravo i mišljenja

1. Court of Justice of the EU (CJEU), Criminal Proceedings against Bodil Lindqvist (C-101/01), ECLI:EU:C:2003:596, 6 November 2003.
2. CJEU, N. S. (C-411/10) v. Secretary of State for the Home Department and M. E. (C-493/10), A. S. M., M. T., K. P., E. H. v. Refugee Applications Commissioner, Minister for Justice, Equality and Law Reform, ECLI:EU:C:2011:865, 21 December 2011.
3. CJEU, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, (Case C-131/12), ECLI:EU:C:2014:317, 13 May 2014.
4. European Court of Human Rights (ECtHR), Klass et al. v. Germany, No. 5029/71, 6 September 1978.
5. ECtHR, Malone v. the United Kingdom, No. 8691/79, 26 April 1985.
6. ECtHR, Sciacca v. Italy, No. 50774/99, 11 January 2005.
7. ECtHR, Uzun v. Germany, No. 35623/05, 2 September 2010.
8. ECtHR, K.U. v. Finland, No. 2872/02, 2 December 2008.
9. ECtHR, Halford v. United Kingdom, 25 June 1997, Izveštaji 1997-III.
10. ECtHR, Copland v. United Kingdom, Br. 62617/00, 3 April 2007.
11. European Data Protection Supervisor, Opinion 7/2015, Meeting the Challenges of Big Data: A Call for transparency, user control, data protection by design and accountability, 19 November 2015.
12. Ombudsman, Decision in case 2004/2013/PMC on the European Commission's handling of an access to documents request relating to the surveillance of the internet by UK intelligence services, Decision of 5 November 2015 and Recommendation of 2 October 2014.
13. Working Party Article 29, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.
14. Working Party Article 29, Opinion 5/2009 on online social networking, WP 163, 12 June 2009.

15. Working Party Article 29, Opinion 01/2010 on the concepts of controller and processor, WP 169, 16 February 2010.
16. Working Party Article 29, Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, 16 May 2011.
17. Working Party Article 29, Opinion 15/2011 on the definition of consent, WP 187, 3 July 2011.
18. Working Party Article 29, Opinion 02/2013 on apps on smart devices, WP202, 27 February 2013.
19. Working Party Article 29, Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013.
20. Working Party Article 29, Opinion 06/2013 on open data and public sector information ('PSI') reuse, WP 207, 5 June 2013.
21. Working Party Article 29, Opinion 05/2014 on Anonymisation Techniques, WP 216, 9 April 2014.
22. Working Party Article 29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 10 April 2014.
23. Working Party Article 29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, WP 223, 16 September 2014.

Smernice, priručnici, dokumenti o politici

1. Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs'), 13 December 2016.
2. Article 29 Working Party, Guidelines on the right to data portability, 13 December 2016.
3. Article 29 Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, 13 December 2016.
4. European Data Protection Supervisor, Monitoring and Ensuring Compliance with Regulation (EC) 45/2001, Policy paper, Brussels, 13 December 2016.
5. Fundamental Rights Agency, Handbook on European law relating to asylum, borders and immigration, 2014.

1. Baldry, Tony, *Hyams, Oliver*, "The Right to Be Forgotten", *1 Essex Court*; <https://1essexcourt.wordpress.com/2014/05/15/the-right-to-be-forgotten/>
2. *Blackmer, W.S.*, "GDPR: Getting Ready for the New EU General Data Protection Regulation", *Information Law Group*, 5 May 2016.
3. Cedric Burton, Laura De Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot and Sára G. Hoffman, The Final European Union General Data Protection Regulation; <https://www.bna.com/final-european-union-n57982067329/#!>
4. Comparative Law in the Reasoning of the ECtHR; http://epubs.surrey.ac.uk/186004/3/Microsoft_Word_-_Working_draft_comparative_law.pdf
5. D. Manolescu, Data protection as a fundamental right; http://effectius.com/yahoo_site_admin/assets/docs/Data_protection_as_a_fundamental_right_Dan_Manolescu_Issue5.16761659.pdf
6. Information Commissioner of Slovenia, Guidelines: Media and the protection of personal data; https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Media_and_the_Protection_of_Personal_Data.pdf
7. Inofficial Consolidated Version After Libe Committee Vote Provided by the Rapporteur Jan Philipp Albrecht, 22 October 2013; <http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf>
8. Irion, Kristina, Yakovleva, Svetlana, and Bartl, Marija, Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements, *Institute for Information Law (IViR), University of Amsterdam*, 22 September 2016.
9. M law group, New draft European data protection regime; http://mlawgroup.de/news/publications/detail.php?we_objectID=227
10. Mühlich, Regina, Expert tips: Get your business ready for GDPR; <https://tresorit.com/blog/expert-tips-business-gdpr-ready/>

11. The Proposed EU General Data Protection Regulation. A guide for in-house lawyers, Hunton & Williams LLP, June 2015, p. 14.
12. Schmitt Judy, Florian Stahl, How the Proposed EU Data Protection Regulation Is Creating Ripple Effect Worldwide, 11 October 2012; https://iapp.org/media/presentations/A12_EU_DP_Regulation_PPT.pdf

Drugo

1. Article 29 Working Party, Rules of procedure, Brussels, 15 February 2010; http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf
2. Article 29 Working Party, WP242 ANNEX – Frequently Asked Questions; http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf
3. Article 29 Working Party, WP243 ANNEX – Frequently Asked Questions; http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf
4. Article 29 Working Party, WP244 ANNEX II – Frequently Asked Questions; http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_annexii_en_40858.pdf
5. *European Commission*, European Commission – Fact Sheet. Questions and Answers – Data protection reform, 21 December 2015; http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
6. European Commission's press release announcing the proposed comprehensive reform of data protection rules, 25 January 2012; http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en
7. European Commission swears oath to respect the EU Treaties, Press release; http://europa.eu/rapid/press-release_IP-10-487_en.htm
8. Presidency of the Council: "Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears

in annex”, 201 p., 11 June 2015; <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>

9. Article 83 (5) of The Council's first reading after the trialogue sets maximum fines to be the highest of 4% of global turnover and 20 million Euro; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT. The Commission adopted the views of the Council's document April 11th 2016, see COM/2016/214/FINAL and ST 5419 2016 ADD 1 – 2012/011 (OLP).

Internet izvori

1. http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU_1.1.6.html (pristupljeno 20. 3. 2017. godine).
2. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046> (pristupljeno 2. 3. 2017. godine).
3. http://ec.europa.eu/justice/data-protection/reform/index_en.htm (pristupljeno 20. 3. 2017. godine).
4. <http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046> (pristupljeno 2. 3. 2017. godine).
5. <http://www.eugdpr.org/key-changes.html> (pristupljeno 2. 3. 2017. godine).
6. https://ec.europa.eu/info/about-european-union/organisational-structure/political-leadership_en (pristupljeno 2. 3. 2017. godine).
7. <https://epic.org/privacy/intl/schrems/> (pristupljeno 2. 3. 2017. godine).
8. http://ec.europa.eu/justice/data-protection/index_en.htm (pristupljeno 2. 3. 2017. godine).
9. http://ec.europa.eu/justice/data-protection/article-29/files/tasks-art-29_en.pdf (pristupljeno 2. 3. 2017. godine).
10. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (pristupljeno 6. 3. 2017. godine).
11. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf (pristupljeno 6. 3. 2017. godine).

12. <http://developer.android.com/wear/index.html> (pristupljeno 6. 3. 2017. godine).
13. <http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results> (pristupljeno 6. 3. 2017. godine).
14. <http://www.dataprotection.ro/servlet/ViewDocument?id=1088> (pristupljeno 18. 3. 2017. godine).
15. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf (pristupljeno 6. 3. 2017. godine).
16. <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/cache/offonce#> (pristupljeno 17. 2. 2017. godine).
17. <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Seurodac> (pristupljeno 17. 2. 2017. godine).
18. <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines> (pristupljeno 17. 2. 2017. godine).
19. <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/cache/offonce#> (pristupljeno 17. 2. 2017. godine).
20. <http://fra.europa.eu/en/about-fra/who-we-are> (pristupljeno 1. 3. 2017. godine).
21. <http://fra.europa.eu/en/survey/2012/eu-midis-european-union-minorities-and-discrimination-survey> (pristupljeno 1. 3. 2017. godine).
22. <http://fra.europa.eu/en/publications-and-resources/data-and-maps/survey-data-explorer-violence-against-women-survey> (pristupljeno 2. 3. 2017. godine).
23. <http://fra.europa.eu/DVS/DVT/lgbt.php> (pristupljeno 1. 3. 2017. godine).
24. <http://fra.europa.eu/DVS/DVT/roma.php> (pristupljeno 1. 3. 2017. godine).
25. <http://fra.europa.eu/en/publication/2013/discrimination-and-hate-crime-against-jews-eu-member-states-experiences-and> (pristupljeno 1. 3. 2017. godine).
26. <http://fra.europa.eu/en/project/2015/fundamental-rights-survey> (pristupljeno 1. 3. 2017. godine).
27. <http://fra.europa.eu/en/theme/hate-crime> (pristupljeno 13. 2. 2017. godine).

28. <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states> (pristupljeno 6. 3. 2017. godine).
29. <http://fra.europa.eu/en/theme/access-justice> (pristupljeno 13. 2. 2017. godine).
30. <http://fra.europa.eu/en/project/2012/children-and-justice> (pristupljeno 13. 2. 2017. godine).
31. <http://fra.europa.eu/en/publication/2012/fundamental-rights-migrants-irregular-situation-european-union> (pristupljeno 15. 2. 2017. godine).
32. <http://fra.europa.eu/en/theme/people-disabilities> (pristupljeno 13. 2. 2017. godine).
33. <http://fra.europa.eu/en/publication/2015/handbook-european-law-child-rights> (pristupljeno 5. 3. 2017. godine).
34. <http://fra.europa.eu/en/publication/2011/handbook-european-non-discrimination-law> (pristupljeno 6. 3. 2017. godine).
35. [http://fra.europa.eu/en/publications-and-resources/publications?title=law&field_fra_publication_type_tid_i18n\[0\]=88](http://fra.europa.eu/en/publications-and-resources/publications?title=law&field_fra_publication_type_tid_i18n[0]=88) (pristupljeno 1. 3. 2017. godine).
36. https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en
37. <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN> (pristupljeno 5. 3. 2017. godine).
38. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (pristupljeno 5. 3. 2017. godine).
39. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=885051> (pristupljeno 7. 3. 2017. godine).
40. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (pristupljeno 5. 3. 2017. godine).
41. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=891362> (pristupljeno 5. 3. 2017. godine).
42. http://ec.europa.eu/dgs/legal_service/arrets/09c092_en.pdf (pristupljeno 5. 3. 2017).

43. <https://www.ombudsman.europa.eu/en/press/introduction-faces> (pristupljeno 5. 3. 2017. godine).
44. <https://www.europol.europa.eu/partners-agreements> (pristupljeno 5. 3. 2017. godine).
45. <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (pristupljeno 27. 2. 2017. godine).
46. <https://www.europol.europa.eu/about-europol/european-migrant-smuggling-centre-emsc> (pristupljeno 27. 2. 2017. godine).
47. <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc> (pristupljeno 27. 2. 2017. godine).
48. <https://www.europol.europa.eu/about-europol/intellectual-property-crime-coordinated-coalition-ipc3> (pristupljeno 27. 2. 2017. godine).
49. <https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net> (pristupljeno 27. 2. 2017. godine).
50. <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0121> (pristupljeno 27. 2. 2017. godine).
51. <http://www.eurojust.europa.eu/about/Partners/Pages/eu-institutions-agencies-and-bodies.aspx> (pristupljeno 27. 2. 2017. godine).
52. <http://www.eurojust.europa.eu/doclibrary/JITs/JITs%20framework/Council%20Document%20establishing%20the%20JITs%20Network/JITs-Council-document-11037-05-EN.pdf> (pristupljeno 27. 2. 2017. godine).
53. <http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/jsb/jsb/The%20Role%20of%20the%20Joint%20Supervisory%20Body%20of%20Eurojust%20%28leaflet%29/Role-of-JSB-EN.pdf> (pristupljeno 27. 2. 2017. godine).

Naslov originala

Nataša Pirc Musar, Tina Kraigher Mišič
DATA PROTECTION AND COMPETENCIES
OF EUROPEAN UNION INSTITUTIONS
Handbook

Izdavač

Poverenik za informacije od javnog značaja
i zaštitu podataka o ličnosti
Bulevar kralja Aleksandra br. 15, 11000 Beograd
Tel.: + 381 11 3408 900
Faks: + 381 11 3343 379
E-mail: office@poverenik.rs
www.poverenik.rs

Za izdavača

Rodoljub Šabić

Prevod

Kongresni servisni centar d.o.o.

Publikacija se objavljuje u okviru Projekta koji se većinski finansira od strane Ministarstva spoljnih poslova Norveške kroz Bilateralni program Kraljevine Norveške za 2015. godinu, dok su sredstva za ovu publikaciju izdvojena iz budžeta Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.

Lektura, dizajn i prelom
Čigoja štampa

Štampa
Čigoja štampa

Tiraž
500 primeraka

ISBN 978-86-919155-5-1

Beograd, 2018.

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

342.738(4-672EU)(035)

ПИРЦ Мусар, Наташа, 1968–

Zaštita podataka i nadležnosti institucija Evropske unije :
priručnik / Nataša Pirc Musar, Tina Kraigher Mišič. – Beograd :
Poverenik za informacije od javnog značaja i zaštitu podataka o
ličnosti, 2018 (Beograd : Čigoja štampa). – 130 str. : ilustr. ; 21 cm

Prevod dela: Data Protection and Competencies of European
Union Institutions. – Podaci o autorima preuzeti iz kolofona.
– Tiraž 500. – Napomene i bibliografske reference uz tekst. –
Bibliografija: str. 121–130.

ISBN 978-86-919155-5-1

1. Крайгхер Мишич, Тина, 1983– [аутор]

а) Право на заштиту података о личности – Европска унија –
Приручници

COBISS.SR-ID 255002636