Zaštita osobnih podataka i nova EU uredba o zaštiti podataka

Marija Boban

Sveučilište u Splitu Pravni fakultet

marija.boban@pravst.hr

Uvod

Za razumijevanje suvremenog informacijskog društva, samih implikacija razvoja suvremenih informacijskih tehnologija na zaštitu osobnih podataka i privatnost te društvenih i kulturnih promjena, nije presudno ono što se može dogoditi, već razlog zašto će se nešto dogoditi. Često se događa da smo svjedoci očekivanih i planiranih promjena, ali i sudionici u procesima uzrokovanim poznatim čimbenicima koji su imali neočekivano velik utjecaj na cjelokupni sociokulturni razvoj. To se do sada uglavnom i događalo. Postoji mišljenje da se „*velike i brze tehničko-tehnološke promjene u posljednjih 150 godina nisu rješavale stare probleme; već se postojeći problemi uvijek odgađaju ili zamjenjuju novima- stari postaju irelevantni, a novi sudbonosni*. [1] Ubrzanim razvojem suvremenih inforamcijskih i komunikacijskih tehnologija kao i novim načinima obrade osobnih podataka, postalo je nužno donošenje novog zakonodavnog okvira koji će osigurati zaštitu prava i temeljnih sloboda pojedinaca u svezi s obradom njihovih osobnih podataka. U svim modelima kroz povijest razvoja informacijske znanosti nedvojbena je činjenica da je obavijest ključni fenomen, entitet, što se razmjenjuje u komunikacijskom procesu čija priroda nikada do kraja pojašnjena: bilo zato što su definicije parcijalne i usmjerene samo na određene vidove ili fragmente komunikacijskih procesa, ili što nikada nije postignut konsenzus o ponuđenim definicijama. [2] Ono što nije bilo sporno u postavkama informacijske znanosti jest to da se pojava i razvoj informacijske znanosti povezuje sa: razmjenom znanja, komunikacijskim medijima te metodama i tehnikama obrade podataka. Ono što je bilo sporno u tim teorijama jest njihova parcijalnost i nekonzistentnost –unatoč (fragmentarnoj) istinitosti njihovih teza. Dakle, izostalo je tumačenje povijesnog razvoja informacijskih funkcija i informacijskog fenomena jer nisu istražene relacije između znanja, komunikacijskih medija informacijskih procedura.[3]

U novoj eri informacijskog društva, većina proizvodnih procesa je automatizirana i pojednostavljena čak i dovedena na razinu upravljanja umjetnom inteligencijom. Tržište je globalizirano i njegovo funkcioniranje je dovedeno na najvišu razinu[4]. Ipak, u duhu gore

[1] Prema TUĐMAN, M., „*Uvod u informacijsku znanost",* Školska knjiga, 1993., str. 177

[2] Sa stajališta informacijske znanosti već od 50-tih godina teoretičari su upozoravali da se obavijest može protumačiti na tehničkoj, semantičkoj i biheviorističkoj razini, odnosno da je fundamentalni problem komunikacije da se na jednoj točci točno ili približno reproducira poruku odabranu u drugoj točci. Same poruke često imaju značenje - što znači da one upućuju na ili su povezane s nekim sistemom s određenim fizičkim ili konceptualnim svojstvima pa su ti semantički vidovi komunikacije irelevantni su za tehnički problem. Međutim , većina je znanstvenika zanemarila činjenicu da se matematička teorija informacija ne bavi semantičkim ni socijalnim aspektima obavijesti, već se oduševila mogućnošću uporabe teorijskih modela za analizu informacijskih i/ili komunikacijskih procesa. Tako i šire TUĐMAN, M., "*Teorija informacijske znanosti"*, Informator, Zagreb, 1990., str. 15

[3]Tako i šire Boban, M., „*Right to privacy and freedom of information in the modern information society",* Proceedings of the Faculty of Law, Split.Vol 49 (2012), No 3 (105); 2012., str. 576-577

[4]Složeni odnosi distribucije moći u suvremenom društvu (uključujući zapadni i istočnjački model) i komunikacijskim sistemima doveli su do razvoja novih modela distribudije moći i informacija putem masovih

navedene teze, jedan od najvećih problema- vezanih uz elementarna ljudska prava čovjeka i njihovo ugrožavanje - dignut je na još višu potenciju[5]. Ljudska su prava postala ključni element političkih dokumenata poput američke Deklaracije o nezavisnosti iz 1776.g. i francuske *Deklaracije o pravima čovjeka i građanina* iz 1789.g. U *Deklaraciji o nezavisnosti* je istaknuto kako su načelo *„svi su ljudi stvoreni jednakima"* i načelo kako vlast *„izvodi svoje pravedne ovlasti iz suglasnosti onih kojima vlada"*samorazumljive istine.[6] Iako ljudska prva nisu bila samorazumljive istine za tisućljeća ljudske povijesti, pa tako ni za današnje suvremeno informacijsko doba. Dapače, tumačenje je puno sličnije mišljenju da su ljudska prava povijesne i socijalne tvorevine.[7] Pregledom cjelokupne europske zakonodavne regulative naglašavaju se sljedeće konvencije i smjernice u pogledu kreiranja zakonske regulative zaštite osobnih podataka i njihove obrade kako slijedi: Europska konvencija o ljudskim pravima . *engl. European Convention on Human Rights* i nadalje *K*onvencijom o kibernetičkom kriminalu - engl. *Convention on Cybercrime*.[8]. Nadalje, otvoreno pitanje sigurnosti i zaštite privatnosti kao temelja informacijske sigurnosti bilo je regulirano najprije *Direktivom 95/46/EC o zaštiti pojedinaca u pogledu obrade osobnih podataka i slobodnog kretanja takvih podataka* (*engl. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data*), Official Journal (Službeni list) L 268, 19/10/1994 str. 0015 – 0021 preuzeta, Narodne novine MU, br. 4/2005 i br. 6/2005– u daljnjem tekstu Smjernica 95/46/EZ).. a zatim *Direktivom EU 2002/58/EC o obradi osobnih podataka i zaštiti privatnosti podataka u elektroničkom komunikacijskom sektoru (*engl. *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*)- Official Journal (Služeni list) L 201 , 31/07/2002 P. 0037 – 0047- *u daljnjem tekstu* Smjernica 2002/58/EC). Daljnjim vremenskim slijedom donesena je i Konvencija 108 (Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka) – *engl. Convention 108 – Protection of individuals with regard to automatic processing of personal data* te dodatni protokol uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka – *engl. Additional Protocol to the Convention 108 - Protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows*..[9] Republika Hrvatska je,

---

medija. Samim time stvara se nova razina političke komunikacije i društvenih promjena u pluralističkom društvu. Dakle, osim dominantne, u svakom društvu postoji i alternativna, politička komunikacija. O tome više, VRENG, F., *„Political communication and social change in pluralist society"*, Informatologia, 40, 2007., 3, str. 189

[5]Tako i šire TUCAK, I., str. 479.

[6] Šire o tome SMERDEL, B., *Ustav Sjedinjenih Američkih Država*/preveo i napisao uvodnu studiju Branko Smerdel, 2. ponovljeno izanje, Osijek, Pan liber, 1994.

[7] Usp. Shlapentoh, D., „*Universalization off the Rejection of Human Rights: Russia's Case*" PREMA BELL; L., S., NATHAN, A. J., PELEG, I., (ur.), „*Negotiating Culture and Human rights*", New York, Columbia University Press, 2001., str.259.

[8] Konvencija o kibernetičkom kriminalu potpisana je u Budimpešti, 23. studnoega 2001. godine. Njeno značenje je, među inim,i u tome što prelazi granice Vijeća Europe, jer su je osim članica toga Vijeća, prihvatile SAD, Kanada, Japan i Južna Afrika. Budući da je Republika Hrvatska supotpisnica dane Konvencije, Zakonom o izmjenama i dopunama Kaznenog zakona – *Narodne novine br. 105/04* tekst Konvencije o kibernetičkom kriminalu postaje dijelom hrvatskog pravnog poretka. Vidi Zakon o izmjenama i dopunama KZ – NN 105/04

[9] Istu Konvenciju potpisala je i Republika Hrvatska 2003. godine dok je Hrvatski sabor ratificirao tu Konvenciju 2005.godine. Konvencija je stupila na snagu 1. listopada 2005.g.zatim i razvojem pravne regulative u području zaštite osobnih podataka koju je usvojila i Republika Hrvatska. Republika Hrvatska je, kao država članica Vijeća Europe, prihvatila odredbe konvencije 108 u pogledu zaštite osobe glede automatizirane obrade osobnih podataka. Sukladno tome, Hrvatski sabor donio je na sjednici 14. travnja 2005. godine Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju

kao država članica Vijeća Europe, prihvatila odredbe konvencije 108 u pogledu zaštite osobe glede automatizirane obrade osobnih podataka. Sukladno tome, Hrvatski sabor donio je na sjednici 14. travnja 2005. godine *Zakon o (ETS br. 108) koje Europskim zajednicama omogućavaju pristupanje ("Narodne novine - Međunarodni ugovori", br. XX/05)* i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka.[10]

Velik iskorak u području zaštite osobnih podatka i inforamcijske sigurnosti predstavlja upravo donošenje nove *Opće uredbe o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka 2016/679 (Opća uredba o zaštiti podataka – dalje GDPR)* i njenim stupanjem na snagu 25. svibnja 2018. godine, kojim se važeća Direktiva 95/46/EC stavlja van snage. Sam GDPRredstavlja bitan napredak u području zaštite osobnih podataka budući da se njom osigurava ujednačeno i jednoobrazno postupanje nadzornih tijela za zaštitu osobnih podataka, što će imati za posljedicu jednostavniju i jednaku zaštitu prava svih pojedinaca u Europskoj uniji i to na način da sam pojam "Uredbe" znači da se izravno primjenjuje u zakonodavni okvir zemalja članica (izuzev u nekolicini pojmova koji se ostavljeni za razradu u nacionalnim zakonodavstvima) za razliku od do sada važeće "Direktive" koja je predstavljala "samo" Smjernice djelovanja. Također, uvode se nove i pojednostavljuju se neke već postojeće definicije, određuju i definiraju novi pojmovi koji do sada nisu bili zakonski definirani, kao biometrijski i genetski podaci, preciznije opisuju postojeći pojmovi, jačaju prava ispitanika te se smanjuju i pojednostavljuju pojedine administrativne obveze voditelja zbirke osobnih podataka, jačaju nadzorne ovlasti te mogućnost izricanja kazni od strane tijela za zaštitu osobnih podataka.

Zaštita osobnih podataka i nova Opća uredba o zaštiti podataka

Uvodno o Općoj uredbi o zaštiti osobnih podataka (GDPR)

Stvaranje jedinstvenog informacijskog prostora odnosno jedinstvenog europskog digitalnog tržišta mora osigurati odgovarajuća svojstva povjerljivosti, cjelovitosti i raspoloživosti različitih vrsta podataka.[11] Primjenom odgovarajućih sigurnosnih standarda na ljude, organizaciju i tehnologiju, mogu se za različite vrste podataka u različitim korisničkim

za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka.

[10] Prema čl.1., st. 2., 3. i 6. članka 3. ETS 108 nalaže da svaka država ili Europske zajednice mogu, pri potpisivanju ili pri polaganju svoje isprave o ratifikaciji, prihvatu, odobrenju ili pristupu, ili kasnije u svako doba, izjavom upućenom glavnom tajniku Vijeća Europe priopćiti da ovu Konvenciju *neće primjenjivati na određene kategorije automatiziranih zbirki osobnih podataka, popis kojih će položiti*. *U taj popis ne smiju, međutim, uključiti kategorije automatiziranih zbirki podataka koje su prema njihovom unutarnjem pravu predmet odredaba o zaštiti podataka*. Slijedom toga, *taj će popis izmijeniti i dopuniti novom izjavom kad god dodatne kategorije automatiziranih zbirki osobnih podataka postanu predmetom odredaba o zaštiti podataka prema njihovom unutarnjem pravu*. Također, obvezuju se da će ovu Konvenciju također *primjenjivati na obavijesti koje se odnose na skupine osoba, udruge, zaklade, društva, korporacije i sva ostala tijela koja izravno ili neizravno čine fizičke osobe, bez obzira na to imaju li ili nemaju takva tijela pravnu osobnost* i da će ovu Konvenciju također primjenjivati na *zbirke osobnih podataka koje nisu predmet automatizirane obrade*. Također, st. 3. navodi da svaka država ili Europske zajednice koje su nekom od izjava predviđenih ranijim točkama b. ili c. st. 2. proširile područje primjene ove Konvencije mogu, spomenutom izjavom, naznačiti da će se takva proširenja primjenjivati samo na određene kategorije zbirki osobnih podataka, popis kojih će se priložiti. *Usp. čl. 1 st. 2., st. 3 i st. 6 čl. 3 ETS 108 NN Međunarodni ugovori", br. XX/05*

[11] O novostima u europskom pravnom okviru vidi više u BOBAN, M., „ePrivacy and new European Data Protection Regime", // International Scientific Conference ESD 2016, Managerial Issues in Modern Business" Warsaw, Poland, 2016. str. 152-159

okruženjima osigurati tražena svojstva sigurnosti.[12] Stoga se odgovarajući sigurnosni standardi propisuju u svim okruženjima koje karakterizira primjena određene vrste podataka. Kada govorimo o vrstama podataka, informacijska sigurnost se prvenstveno odnosi na podatke koji predstavljaju *„tajnu"*[13] odnosno podatke kojima se određuje određeni *stupanj tajnosti* odnosno *klasifikacije podatka* kako bi se zaštitio njihov sadržaj dok se zaštita osobnih podataka definira šire i odnosi se na zaštitu osobnosti i zaštitu privatnosti, osobito kada se radi o kategoriji "posebno osjetljivih podataka" kao što su u pravilu podatci u zdravstvu.

Dodatnu problematiku kod pojma digitalnog tržišta predstavlja i sama definicija pojma „digitalizacije" koja, prema Castellsu, predstavlja okosnicu razvoja informacijske superprometnice te otvara kompleksnost zaštite privatnosti i informacijske sigurnosti. Liberalizacija se pak prvenstveno odnosi na otvorenost neograničenog komunikacijskog prostora s pratećim procesom kulturne globalizacije. Globalizacija pak, uz podršku informacijskih i komunikacijskih tehnologija i otvorenog globalnog prostora, svjetske trendove premješta u lokalne okvire.[14] Nadalje, sama otvorenost arhitekture Interneta i njegov kontinuirani razvoj u kojemu su korisnici bili istovremeno i kreatori i pridonosili njegovom daljnjem razvoju, bile su njegove glavne snage razvoja.[15] Nastavno na takav nezaustavljivi trend informacijskog društva kojim se unaprjeđuje kvaliteta komunikacija, oplemenjuje razvoj tehnologija, postavlja se i važan zadatak – uspostavljanje modela zaštite podataka, osobito zaštite osobnih podataka, najvrjednijeg dijela osobnosti i koncepta individualnosti nasuprot globalnoj univerzalnosti predstavlja jedan od ključnih ciljeva reforme regulative zaštite podataka koja je stupila na snagu 27. travnja 2016.g. Nakon više od 7 godina od početne inicijative i četiri godine pregovora, novi europski okvir za zaštitu osobnih podataka konačno je usvojen u travnju 2016. godine. Opća EU uredba o zaštiti podataka 2016/679, poznatija pod nazivom GDPR – General Data Protection Regulation, unosi velike promjene u načine upravljanja osobnim podacima i izravno se primjenjuje na sve organizacije koje raspolažu osobnim podacima EU građana. Nadalje, kao članica Europske unije, Hrvatska je obvezna uskladiti svoje zakonodavstvo s novodonesenom regulativom EU u području zaštite podataka, kao i sve ostale članice EU, do 2018.g. [16] Značaj ove reforme proizlazi upravo iz njenog temeljnog cilja donošenja a to je determinirati granice i maksimalno zaštititi protok podataka s naglaskom na obradu osobnih podataka i zaštitu privatnosti građana na području Europske unije u suvremenom informacijskom društvu čime

[12] Prema DEBAR, H., KHEIR, N., CUPPENS-BOULAHIA, N., CUPPENS, F., *„Service Dependencies in Inofrmation Systems Security*", *Computer Network Security*: *Proceedings of 5th International Conference, on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010*, St. Petersburg, Russia, September 8.-10. 2010, str. 1

[13] Prema čl. 2 *Zakona o zaštiti tajnosti podataka Narodne novine 108/1996* (koji je prestao važiti sa donošenjem novog Zakona o tajnosti podataka) „*tajna je podatak koji je zakonom, drugim propisom, općim aktom ili drugim aktom nadležnog tijela donesenim na temelju zakona, određen tajnim*.". Usp. Zakon o zaštiti tajnosti podataka NN 108/96 čl. 2

[14] „Preduvjet za ovakav razvoj Interneta bila je otvorena, decentralizirana, interaktivna mrežna arhitektura, zatim mrežni protokoli koji također moraju biti otvoreni i koji se mogu jednostavno modificirati, te institucije/strukture upravljanja i razvoja Interneta koji moraju biti u skladu s principima otvorenosti i suradnje kako ga ne bi kočile." Usp. CASTELLS, M., „*The Internet Galaxy: Reflections on the Internet, Business, and Society*", OxfordUniversity Press, 2001. str. 28-29

[15] O tome vidi šire u CERF, V. G., KAHN, R. E., "*A protocol for packet network interconnection",* IEEE Trans. Comm. Tech., vol. COM-22, V 5, May 1974., str. 627-641

[16]Službeno priopćenje Europskog parlamenta na temu usklađivanja zakonodavnog paketa dostupno je pod poveznicom: http://www.europarl.europa.eu/news/hr/news-room/20160407IPR21776/Reforma-za%C5%A1tite-podataka-EP-odobrio-nova-pravila (01. 12. 2017.)

se cjelokupna pravna i sigurnosna zaštita dižu na višu razinu sigurnosti i zaštite u suvremenom informacijskom društvu.[17]

Uz navedenu Opću uredbu, sastavni dio usvojenog zakonodavnog paketa je i Direktiva o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka. Tom će se Direktivom ujednačiti zaštita osobnih podataka koje obrađuju pravosudna i policijska tijela u državama članicama Europske unije. Ista jasno definira mogućnosti obrade osobnih podataka ispitanika, uključujući njihovo iznošenje u treće zemlje, pri čemu se osiguravaju visoki standardi zaštite pojedinaca razmjerno s potrebama provedbe odgovarajućih policijskih i pravosudnih postupaka. Ovom Direktivom jasno se određuje nadzor neovisnog tijela za zaštitu osobnih podataka nad obradom istih.[18] Važno je istaknuti kako GDPR zamjenjuje trenutnu EU direktivu te stupa na snagu danom donošenja i direktno se primjenjuje u svim državama članicama EU. Za nadzor će vjerojatno zadužena Agencija za zaštitu osobnih podataka (AZOP) s mogućnošću izmjene naziva budući da je mogućnost prilagodbe određenih dijelova ipak je ostavljena u nacionalnom zakonodavstvu zaključno s 25. svibnja 2018. kada se GDPR počinje primjenjivati! Sa sobom donosi značajne promjene u pravilima koja definiraju osobne podatke i kako se oni „smiju“ obrađivati.

Nova definicija „osobnog podatka“ prema GDPR-u

Podsjetimo, prvi Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12 – dalje ZZOP) u Hrvatskoj je donesen još 2003. godine (zadnje izmjene i dopune 2012.) a ova Uredba je prvi odmak u zakonskoj definiciji na razini Europske unije još 1995. godine. Iscrpna pravna definicija osobnog podatka dana je u ZZOP-u prema kojem *„osobni podatak predstavlja svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati odnosno osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.“* (ZZOP čl. 2. st. 1) Nova Uredba dodaje i doponu i to izrijekom dopunom pravne definicijie koja uključuje i podatke: “*o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;“* čime se po prvi put definiraju (i zakonski uređuju!) biometrijski podaci kao osobni podaci te se uvodi pojam *„mrežni identifikator“* kao i sama obrada *„lokacije“!* (GDPR, čl. 4 st. 1)[19]. Kao i ranije, ključan dio za obradu osobnih podataka jest “privola” osobe na korištenje njenih osobnih podataka koja se smatra jasnim činom odobrenja. Naime, *„privola” ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim*

[17] Detaljno o Uredbi i sadržaju Uredbe te značaju za zaštitu osobnih podataka vidi u Boban, M., (2016) „*Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world“,* 16th International Scientific Conference on Economic and Social Development “The Legal Challenges of Modern World”: Book of Proceedings/ Primorac, Ž.; Bussoli, C.; Recke, N. (ur.). Varaždin; Split; Koprivnica: Development and Entrepreneurship Agency; Faculty of Law; University North, Koprivnica, 2016, str. 191 – 202

[18] Poveznica na Opću uredbu o zaštiti osobnih podataka dostupna je pod: http://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR (01. 12. 2017.)

[19] Definicija osobnih podataka prema Uredbi GDPR: „*osobni podaci” znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;“* Vidi GDPR, čl. 4. st. 11

on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose; (GDPR, čl. 4 st. 11). Novost predstavlja činjenica da su u slučaju proboja sigurnosti podataka tvrtke dužne obavijestiti nadležne službe, ali i pojedinca čiji su osobni podaci povrijeđeni što ranije nije bio slučaj.

Obrada posebnih kategorija osobnih podataka – s naglaskom na "e-zdravlje"

Podsjetimo, ključan dio ZZOP-a i Uredbe svakako je i sama definicija „*obrade podataka*" koja prema GDPR-u: *"znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje." (*GDPR, čl. st. 2) Sama obrada podataka i privola ključni su dio kako ZZOP-a tako i GDPR-a i značajni pojmovno za svaki oblik obrade podataka kako u javnom tako i u privatnom sektoru. S posebnim naglaskom na "osjetljive podatke". Naime, Uredba državama članicama pruža prostor za djelovanje kako bi bolje odredile njezina pravila uključujući obradu posebnih kategorija osobnih podataka („osjetljivi podaci"). U tom smislu ovom se Uredbom ne isključuje pravo države članice kojim se utvrđuju okolnosti posebnih situacija obrade, što uključuje preciznije određivanje uvjeta pod kojima je obrada osobnih podataka zakonita. (GDPR, Preambula, točka 10)

Prema Uredbi, *posebne kategorije osobnih podataka* koje zaslužuju veći stupanj zaštite trebale bi se obrađivati samo u svrhe povezane sa zdravljem radi ostvarivanja tih svrhâ u korist pojedinaca i društva u cjelini, pogotovo u kontekstu upravljanja uslugama i sustavima zdravstvene ili socijalne skrbi, u što se ubraja i obrada takvih podataka koju u svrhu kontrole kvalitete, informacija o upravljanju i općeg nacionalnog i lokalnog nadzora sustava zdravstvene ili socijalne skrbi provode uprava i središnja nacionalna tijela nadležna za zdravlje i u svrhu osiguravanja kontinuiteta zdravstvene ili socijalne skrbi i prekogranične zdravstvene skrbi ili u svrhe zdravstvene zaštite, nadzora i uzbunjivanja, ili u svrhe arhiviranja u javnom interesu, u svrhe znanstvenih ili povijesnih istraživanja ili u statističke svrhe utemeljene na pravu Unije ili pravu države članice i čime treba ostvariti cilj od javnog interesa, kao i za studije koje se provode u javnom interesu u području javnog zdravlja. Stoga se Uredbom utvrđuju usklađeni uvjeti za obradu posebnih kategorija osobnih podataka koji se odnose na zdravlje, za posebne potrebe, osobito kada obradu takvih podataka za određene zdravstvene svrhe provode osobe koje podliježu zakonskoj obvezi čuvanja poslovne tajne. Pravom Unije ili pravom države članice trebalo bi predvidjeti specifične i primjerene mjere za zaštitu temeljnih prava i osobnih podataka pojedinaca. Također, državama članicama trebalo bi omogućiti zadržavanje ili uvođenje dodatnih uvjeta, uključujući ograničenja, u vezi s obradom genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje. Međutim, to ne bi trebalo spriječiti slobodan protok osobnih podataka unutar Unije ako se ti uvjeti primjenjuju na prekograničnu obradu takvih podataka. (GDPR, Preambula, točka 53)

Posebnu kategoriju predstavljaju upravo osobni podaci djece gdje je ponajprije postavljena dobna granica 16 godina al i mogućnost predviđanja niže dobne granice za davanje privole za obradu osobnih podataka djece i do 13 godina.[20] Države članice mogu u te svrhe zakonom

[20] Sukladno čl. 8 GDPR-a pod nazivom Uvjeti koji se primjenjuju na privolu djeteta u odnosu na usluge informacijskog društva u st. *1. „Kada se primjenjuje članak 6. stavak 1. točka (a), u pogledu nuđenja usluga informacijskog društva izravno djetetu, obrada osobnih podataka djeteta zakonita je ako dijete ima najmanje 16 godina. Ako je dijete ispod dobne granice od 16 godina takva je obrada zakonita samo ako i u mjeri u kojoj je*

predvidjeti nižu dobnu granicu, pod uvjetom da takva niža dobna granica nije niža od 13 godina. (GDPR, čl. 8. st. 1.) Postoje dodatni uvjeti koje treba zadovoljiti kada se zahtjev za brisanje odnosi na osobne podatke djece, osobito u online okruženjima. Osobito je značajan element "privole" – osoba je kao dijete dala privolu za obradu podataka, no nakon nekoliko godina zatražila je brisanje. Osoba ima opravdani razlog za brisanjem podataka, jer kao dijete, za vrijeme davanja privole, nije mogla biti u potpunosti svjesna rizika koji su uključeni u proces obrade. [21] Ovo se osobito odnosi na obradu podataka u e-zdravstvu čime će se uistinu utjecati na procedure kako u području pisane suglasnosti tako i u obradi informacija o "e-zapisima" djece i njihovog prosljeđivnja roditeljima. Važan aspekt biti će pisana privola (suglasnost) djeteta.[22]

Obrada i javni pristup službenim dokumentima

Tijelo javne vlasti, javno ili privatno tijelo može otkriti osobne podatke iz službenih dokumenata koje posjeduje to tijelo javne vlasti ili to tijelo u svrhu obavljanja zadaće u javnom interesu u skladu s pravom Unije ili pravom države članice koje se primjenjuje na to tijelo javne vlasti ili to tijelo kako bi se uskladio javni pristup službenim dokumentima s pravom na zaštitu osobnih podataka u skladu s ovom Uredbom. (GDPR, čl. 86)

Obrada nacionalnog identifikacijskog broja

Države članice mogu dodatno utvrditi posebne uvjete za obradu nacionalnog identifikacijskog broja ili bilo kojeg drugog identifikatora opće primjene. U tom se slučaju nacionalni identifikacijski broj ili bilo koji drugi identifikator opće primjene upotrebljava samo uz primjenu odgovarajućih zaštitnih mjera u pogledu prava i sloboda ispitanika u skladu s ovom Uredbom. (GDPR, čl. 87)

Obrada u kontekstu zaposlenja

Države članice mogu zakonom ili kolektivnim ugovorima predvidjeti preciznija pravila s ciljem osiguravanja zaštite prava i sloboda u vezi s obradom osobnih podataka zaposlenika u kontekstu zaposlenja, osobito za potrebe zapošljavanja, izvršavanja ugovora o radu, što uključuje ispunjavanje zakonski propisanih obveza ili obveza propisanih kolektivnim ugovorima, za potrebe upravljanja, planiranja i organizacije rada, jednakosti i različitosti na radnome mjestu, zdravlja i sigurnosti na radu, zaštite imovine poslodavca ili klijenta i za potrebe ostvarenja i uživanja prava i koristi iz radnog odnosa, na individualnoj ili kolektivnoj osnovi, te za potrebe prestanka radnog odnosa. (GDPR, čl. 88, st. 1.)

Pravo na brisanje - „pravo na zaborav"

Značajni iskorak GDPR-a u kontekstu zaštite osonbih podataka jest "*pravo na brisanje*", poznato i kao *„pravo na zaborav*" (engl. *right to be forgotten)* sukladno čl. 17 GDPR-a. Načelo ovog prava je omogućiti pojedincima da zatraže brisanje ili uklanjanje osobnih podataka ukoliko nema uvjerljivog razloga za njihovu obradu. Sukladno čl. 17 st. 1 GDPR.a Osoba ima pravo ishoditi od voditelja obrade: "*brisanje osobnih podataka koji se na njega*

privolu dao ili odobrio nositelj roditeljske odgovornosti nad djetetom." (GDPR, čl. 8 st. 1)

[21] U tom slučaju, sukladn Uredbi, „*Voditelj obrade mora uložiti razumne napore u provjeru je li privolu u takvim slučajevima dao ili odobrio nositelj roditeljske odgovornosti nad djetetom, uzimajući u obzir dostupnu tehnologiju.*" (GDPR, čl. 8 st. 3)

[22] Šire o tome vidi u ADAMS, S., PURTOVA, N.,LEENES, R., „*Under Observation: The Interplay Between eHealth and Surveillance"*, Springer, 2016. , str. 131

odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta: (a) osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni; (b) ispitanik povuče privolu na kojoj se obrada temelji u skladu s člankom 6. stavkom 1. točkom (a) ili člankom 9. stavkom 2. točkom (a) i ako ne postoji druga pravna osnova za obradu; (c) ispitanik uloži prigovor na obradu u skladu s člankom 21. stavkom 1. te ne postoje jači legitimni razlozi za obradu, ili ispitanik uloži prigovor na obradu u skladu s člankom 21. stavkom 2.; (d) osobni podaci nezakonito su obrađeni; (e) osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili prava države članice kojem podliježe voditelj obrade; (f) osobni podaci prikupljeni su u vezi s ponudom usluga informacijskog društva iz članka 8. stavka 1. (GDPR, čl. 17. st. 1.) Primjenjuje se ukoliko osobni podaci više nisu potrebni za svrhu za koju su se prikupljali/koristili, kada ispitanik povuče suglasnost, kada se ispitanik protivi obradi i ne postoji legitiman razlog za nastavak obrade, ukoliko su podaci protupravno obrađeni, ukoliko se osobni podaci moraju izbrisati kako bi se udovoljilo zakonskoj obvezi te ako se radi o osobnim podacima koji se odnose na djecu u svezi s ponudom usluga informacijskog društva. U slučaju ako je voditelj obrade javno objavio osobne podatke i dužan je u skladu sa stavkom 1. obrisati te osobne podatke, uzimajući u obzir dostupnu tehnologiju i trošak provedbe, voditelj obrade poduzima razumne mjere, uključujući tehničke mjere, kako bi informirao voditelje obrade koji obrađuju osobne podatke da je ispitanik zatražio od tih voditelja obrade da izbrišu sve poveznice do njih ili kopiju ili rekonstrukciju tih osobnih podataka. (GDPR, čl. 17. st. 2.). Također, u članku 16. Uredba predviđa i *"pravo na ispravak"* tako da osoba može zatražiti ispravak[23] i/ili brisanje osobnih podataka ako su podaci nepotpuni, netočni ili neažurni.

Nadalje zakonodavac je postavio i uvjete prema kojima zahtjev za brisanjem može biti odbijen i to u slučajevima kada se podaci obrađuju da bi se ostvarilo pravo na slobodu izražavanja i informiranja, da bi se udovoljilo zakonskoj obvezi obavljanja zadaća od javnog interesa ili službenih ovlasti, za svrhe javnog zdravstva – a u interesu javnosti, za arhiviranje u svrhu javnog interesa, znanstvenog/povijesnog istraživanja ili u statističke svrhe te u svrhu postavljanja, ostvarivanja ili obrane pravnih zahtjeva. (GDPR, čl. 3 st. 17.)

Predviđena je i *obveza izvješćivanja u vezi s ispravkom ili brisanjem osobnih podataka ili ograničenjem obrade* koja voditelji obrade nalaže priopćivanje svakog ispravka ili brisanja osobnih podataka ili ograničenje obrade provedeno u skladu s člankom 16., člankom 17. stavkom 1. i člankom 18. svakom primatelju kojem su otkriveni osobni podaci, osim ako se to pokaže nemogućim ili zahtijeva nerazmjeran napor. Nadalje, voditelj obrade obavješćuje osobe o tim primateljima ako to osoba zatraži. (GDPR, čl. 19.) To u praksi znači kako GDPR pojačava pravo na brisanje pojašnjavanjem – organizacije u online okruženju koje javno objavljuju osobne podatke trebaju obavijestiti druge organizacije koje obrađuju osobne podatke za brisanje veza, kopiranja ili replikacije osobnih podataka o kojima je riječ.

Pseudonimizacija

Osim brisanja tu je i pitanje obveze *"pseudonimizacije*" podataka što znači obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci

[23] Sukladno čl. 16. GDPR-a Pravo na ispravak: „*Ispitanik ima pravo bez nepotrebnog odgađanja ishoditi od voditelja obrade ispravak netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave*." (čl. 16 GDPR)

ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi. (GDPR, čl. 4. st. 5.) Načela zaštite podataka trebala bi se primjenjivati na sve informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Osobne podatke koji su pseudonimizirani, a koji bi se mogli pripisati nekom pojedincu uporabom dodatnih informacija trebalo bi smatrati informacijama o pojedincu čiji se identitet može utvrditi. Kako bi se odredilo može li se identitet pojedinca utvrditi, trebalo bi uzeti u obzir sva sredstva, poput primjerice selekcije, koja voditelj obrade ili bilo koja druga osoba mogu po svemu sudeći upotrijebiti u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca. Kako bi se utvrdilo je li po svemu sudeći izgledno da se upotrebljavaju sredstva za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir sve objektivne čimbenike, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir i tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj. (Preambula, točka 25)[24]

Procjena učinka na zaštitu podataka i prethodno savjetovanje

Postupak "psudonimizracije" do sada nije bio zakonski zahtjev i predstavlja izrazit izazov i u području "e-zdravlja" budući da se radi o velikoj količini "osobnih podataka" koji ulaze u kategoriju "osjetljivih podataka" te će u svakom slučaju zahtijevati i dodatnu "procjenu učinka" koju propisuje GDPR. Naime, voditelj obrade trebao bi provesti procjenu učinka na zaštitu podataka prije obrade radi procjene osobite vjerojatnosti i ozbiljnosti visokog rizika, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade te izvore rizika.[25] Ta bi procjena učinka trebala posebno uključivati mjere, zaštitne mjere i mehanizme predviđene za umanjivanje tog rizika, za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s ovom Uredbom. (GDPR, Preambula, točka 90) Procjena učinka na zaštitu podataka osobito bi se trebala provoditi kada se osobni podaci obrađuju radi donošenja odluka o određenim pojedincima na temelju bilo kakve sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na izradi profila iz tih podataka ili na temelju obrade posebnih kategorija osobnih podataka, biometrijskih podataka ili podataka o kaznenim osudama i kažnjivim djelima ili povezanim mjerama sigurnosti. Procjena učinka na zaštitu podataka jednako je potrebna za opsežno praćenje javno dostupnih područja, posebno ako se upotrebljavaju optičko-elektronički uređaji, ili za bilo koje druge postupke za koje nadležno nadzorno tijelo smatra će obrada vjerojatno dovesti do visokog rizika za prava i slobode ispitanika, osobito zato što se njima ispitanike sprečava u ostvarivanju prava ili upotrebi usluge ili ugovora, ili zato što se opsežna obrada provodi sustavno. Obradu osobnih podataka ne bi trebalo smatrati opsežnom ako se odnosi na osobne podatke pacijenata ili klijenata pojedinih liječnika, zdravstvenih djelatnika ili odvjetnika. U takvim slučajevima procjena učinka na zaštitu podataka ne bi trebala biti obvezna. (GDPR, Preambula, točka 91) U nekim okolnostima može biti razumno i ekonomično da procjena učinka na zaštitu podataka obuhvaća više od jednog projekta i tematski šire područje, na primjer ako tijela javne vlasti ili javna tijela namjeravaju uspostaviti zajedničku aplikaciju ili platformu za obradu ili ako nekoliko voditelja obrade namjerava uvesti zajedničku aplikaciju ili okruženje za obradu u cijeli jedan industrijski sektor ili segment ili za horizontalnu djelatnost široke uporabe. (GDPR, Preambula, točka 92)

Nadalje, Uredba eksplicitno navodi ukoliko postoji vjerojatnost da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade,

[24] Sukladno tekstu preambule Uredbe. Vidi GDPR, t. 25, str. 5

[25] O metodlogiji procjene rizika vidi više u BOBAN, M., "*Krizno upravljanje i upravljanje sigurnošću informacijskih sustava kao temeljni oblici prevencije računalnog kriminaliteta"* // 4th International Scientific and Professional Conference 'Police College Research Days in Zagreb, Zagreb, 2015. str. 27-52

prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka. (GDPR, čl. 35. st. 1.) Također, u istom stvaku navodi se da se jedna procjena može odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike. Isto tako, pri provođenju procjene učinka na zaštitu podataka voditelj obrade traži savjet od službenika za zaštitu podataka u organizacijama u kojima je on imenovan. (GDPR, čl. 35. st. 2.).

Prema GDPR-u, procjena učinka na zaštitu podataka obvezna je osobito u slučaju: (a) sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca; (b) opsežne obrade posebnih kategorija osobnih podataka iz članka 9. stavka 1. ili podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.; ili (c) sustavnog praćenja javno dostupnog područja u velikoj mjeri. (GDPR, čl. 35. st. 3.) Nadzorno tijelo, sukladno Uredbi, uspostavlja i javno objavljuje popis vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka u skladu sa stavkom 1.[26] (GDPR, čl. 35. st. 4.) Nacionalno Nadzorno tijelo priopćuje te popise Europskom odboru za zaštitu podataka sukladno članku 68. GDPR-a. Sama procjena učinka na zaštitu podataka sadrži barem:

(a) sustavan opis predviđenih postupaka obrade i svrha obrade, uključujući, ako je primjenjivo, legitimni interes voditelja obrade;

(b) procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama;

(c) procjenu rizika za prava i slobode ispitanikâ iz stavka 1.; i

(d) mjere predviđene za rješavanje problema rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s ovom Uredbom, uzimajući u obzir prava i legitimne interese ispitanika i drugih uključenih osoba. (GDPR, čl. 35. st. 7.)[27]

Upravo poglavlje *"procjene učinka*" izazvalo je najviše interesa kod donošenja GDPR-a budući da dosadašnji važeći Zakon o zaštiti osobnih podataka nije uvodio obvezu procjene rizika i sigurnosti zaštite podataka već samo prijavu zbirki podataka. Na tom tragu ako obrada u skladu s člankom 6. stavkom 1. točkom (c) ili (e) GDPR-a ima pravnu osnovu u pravu Unije ili pravu države članice kojem voditelj obrade podliježe, ako su tim pravom uređuju posebni postupci obrade ili skupina dotičnih postupaka te je procjena učinka na zaštitu podataka već provedena kao dio opće procjene učinka u kontekstu donošenja pravne osnove, stavci od 1. do 7. članka 35. GDPR-a se ne primjenjuju osim ako države članice smatraju da je potrebno provesti takvu procjenu prije aktivnosti obrade.

Prije obrade podataka Uredba navodi potrebu savjetovanja voditelja obrade s nadzornim tijelom i to u slučaju ako se procjenom učinka na zaštitu podataka iz članka 35. pokazalo da bi, ukoliko voditelj obrade ne donese mjere za ublažavanje rizika, obrada dovela do visokog rizika. (GDPR, čl. 36 st. 1.) Ako nadzorno tijelo smatra da bi se namjeravanom obradom

[26] Prije usvajanja popisa iz stavaka 4. i 5. čl. 35 GDPR-a, nadležno nadzorno tijelo primjenjuje mehanizam konzistentnosti iz članka 63. kada takvi popisi obuhvaćaju aktivnosti obrade koje su povezane s ponudom robe ili usluga ispitanicima ili s praćenjem njihova ponašanja u nekoliko država članica ili koje mogu znatno utjecati na slobodno kretanje osobnih podataka unutar Unije. Vidi GDPR, čl. 6.

[27] Detaljnije o procjeni učinka i proceni rizika vidi u ČIZMIĆ, D., BOBAN, M., ZLATOVIĆ, D., „*Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost",* Sveučilište u Splitu Pravni fakultet, Split, 2016. Vidi i BOBAN, M., *"Upravljanje sigurnosnim rizicima i krizno upravljanje u mrežnoj komunikaciji* "// Dani kriznog upravljanja 2014., Zagreb, 2014. str. 549-572

kršila Uredba, osobito ako voditelj obrade nije u dovoljnoj mjeri utvrdio ili umanjio rizik, nadzorno tijelo u roku od najviše osam tjedana od zaprimanja zahtjeva za savjetovanje pisanim putem savjetuje voditelja obrade i, prema potrebi, izvršitelja obrade, te može iskoristiti bilo koju od svojih ovlasti iz članka 58. Taj se rok može prema potrebi produžiti za šest tjedana, uzimajući u obzir složenost namjeravane obrade. Nadzorno tijelo u roku od mjesec dana od zaprimanja zahtjeva obavješćuje voditelja obrade, i, prema potrebi, izvršitelja obrade o svakom takvom produljenju i o razlozima odgode. Ti se rokovi mogu suspendirati sve dok nadzorno tijelo ne dobije informacije koje je moglo zatražiti u svrhe savjetovanja. (GDPR, čl. 36. st. 2.)

Službenik za zaštitu podataka

Kako bi se osigurala usklađenost s GDPR-m nužno su potrebne stručne osobe koje razumiju zahtjeve GDPR-a i koje su educirane za planiranje, implementaciju i održavanje usklađenosti organizacije prema samoj Uredbi. Na tom tragu, stupanjem GDPR-a na snagu, mnoge tvrtke imaju obvezu imenovanja kvalificiranog službenika za zaštitu podataka (eng. Data Protection Office – DPO) koji će odgovarati izravno Upravi. [28] (GDPR, čl. 37.) Pri tom, ne navodi se eksplicitno struka DPO-a ali prema zahtjevima sustava osoba mora poznavaati i pravni i tehnološki aspekt obrade osobnih podataka. Nadalje, sama obrada mora bit i troškovno isplativa (ekonomična) te u skladu s pravnim zahtjevima Uredbe i samim mogućnostima organizacije što se ostvaruje kroz savjetovanje s nadzornim tijelom. Također, službenik za izvršavanje djeluje neovisno u izvršenju svojih obveza i odgovara direktno upravi kako je i izrečeno u čl. 38 GDPR-a.[29] Nadalje, grupa poduzetnika može imenovati jednog službenika za zaštitu podataka pod uvjetom da je službenik za zaštitu podataka lako dostupan iz svakog poslovnog nastana. (GDPR, čl. 37. st. 2.) Isto tako ako je voditelj obrade ili izvršitelj obrade tijelo javne vlasti ili javno tijelo, za nekoliko takvih vlasti ili tijela može se imenovati jedan službenik za zaštitu podataka, uzimajući u obzir njihovu organizacijsku strukturu i veličinu. (GDPR, čl. 37. st. 3.) Vezano uz kvalifikacije službenika za zaštitu podataka Uredba propisuje kako se službenik za zaštitu podataka imenuje na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja zadaća iz članka 39 GDPR-a. (GDPR, čl. 37. st. 5.) Isto tako, službenik za zaštitu podataka može biti član osoblja voditelja obrade ili izvršitelja obrade ili obavljati zadaće na temelju ugovora o djelu. (GDPR, čl. 37. st. 6.)

Uz osnovno razumijevanje procesa i klasifikacije službenik za zaštitu podataka obavlja najmanje sljedeće zadaće: (a) informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka; (b) praćenje poštovanja ove Uredbe te drugih odredaba Unije ili države članice o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti,

[28] Sukladno čl. 37 st. 1 GDPR-a voditelj obrade i izvršitelj obrade imenuju službenika za zaštitu podataka i to: *„u svakom slučaju u kojem: (a) obradu provodi tijelo javne vlasti ili javno tijelo, osim za sudove koji djeluju u okviru svoje sudske nadležnosti, (b) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri, ili (c) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka na temelju članka 9. i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.“* Prema GDPR, čl. 37. st. 1.

[29] Prema članku 38. st. 3. GDPR-a: *Voditelj obrade i izvršitelj obrade osiguravaju da službenik za zaštitu podataka ne prima nikakve upute u pogledu izvršenja tih zadaća. Voditelj obrade ili izvršitelj obrade ne smiju ga razriješiti dužnosti ili kazniti zbog izvršavanja njegovih zadaća. Službenik za zaštitu podataka izravno odgovara najvišoj rukovodećoj razini voditelja obrade ili izvršitelja obrade.“(*GDPR, čl. 38. st. 3)

podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije; (c) pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35.; (d) suradnja s nadzornim tijelom; (e) djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. te savjetovanje, prema potrebi, o svim drugim pitanjima. (GDPR, čl. 39. st. 1.) Službenik za zaštitu podataka pri obavljanju svojih zadaća vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade. (GDPR, čl. 39. st. 2.)

Sankcije GDPR-a - izricanje upravnih novčanih kazni

Počevši s postroženim pravilima obrade, najvažniji je naglasak na činjenici kako se pravno jača snaga "nadzornog tijela" te Uredba predviđa kako bi se ojačale i uskladile upravne sankcije za kršenje ove Uredbe, svako nadzorno tijelo trebalo bi imati ovlasti izricati upravne novčane kazne. Nadalje, u Uredbi se eksplicitno se objašnjavaju kršenja te postavlja gornja granica i kriteriji za određivanje povezanih upravnih novčanih kazni, što bi za svaki pojedinačni slučaj trebalo odrediti nadležno nadzorno tijelo, uzimajući u obzir sve bitne okolnosti posebne situacije, vodeći računa osobito o prirodi, težini i trajanju kršenja i njegovim posljedicama te mjerama poduzetim da bi se osiguralo poštovanje obveza iz ove Uredbe te spriječile ili ublažile posljedice kršenja.[30] Nepoštivanje odredbi Uredbe povlači kazne i to drakonske - do 4% ukupnog godišnjeg prometa na svjetskoj razini ili do 20 milijuna eura, koja god vrijednost bude viša.[31] Za razliku od ranije, odnositi će se na sve tvrtke koje posluju na području Europske unije (a ne samo one koje su registrirane u EU!) Ne dovodeći u pitanje korektivne ovlasti nadzornih tijela iz članka 58. stavka 2. svaka država članica može utvrditi pravila mogu li se i u kojoj mjeri tijelima javne vlasti ili tijelima s poslovnim nastanom u toj državi članici izreći upravne novčane kazne. (GDPR, čl. 83. st. 7.) U slučaju lakšeg kršenja ili ako bi moguća novčana kazna nerazmjerno opteretila fizičku osobu, umjesto novčane kazne može se izdati upozorenje. Međutim, posebna bi se pozornost trebala posvetiti naravi, ozbiljnosti i trajanju kršenja, namjeri kršenja, mjerama poduzetim za ublažavanje pretrpljene štete, stupnju odgovornosti ili svim relevantnim prethodnim kršenjima, načinu na koji je nadzorno tijelo doznalo za kršenje, usklađenosti s mjerama naloženima protiv voditelja obrade ili izvršitelja obrade, pridržavanju kodeksa ponašanja te svakom drugom otegotnom ili olakotnom čimbeniku. Propisivanje sankcija, uključujući upravne novčane kazne, trebalo bi podlijegati odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom, uključujući i učinkovitu sudsku zaštitu i pravilno postupanje. (GDPR, Preambula, točka 148.) Države članice trebale bi imati mogućnost propisati pravila o kaznenim sankcijama za kršenja ove Uredbe, uključujući i kršenja nacionalnih pravila donesenih na temelju ove Uredbe i unutar njezinih granica. Te kaznene sankcije mogu obuhvaćati i oduzimanje dobiti stečene kršenjem ove Uredbe. Međutim, izricanje kazni za povrede takvih nacionalnih pravila i upravnih sankcija ne bi smjelo dovesti do kršenja načela ne bis in idem, kako ga tumači Europski sud (GDPR, Preambula, točka 149.). Također, kada se upravne kazne izriču poduzetniku, poduzetnik bi se u te svrhe trebao shvatiti poduzetnik u skladu s člancima 101. i 102. UFEU-a. Ako su upravne kazne izrečene osobama koje nisu poduzetnik, prilikom razmatranja odgovarajućeg iznosa novčane kazne nadzorno tijelo trebalo bi uzeti u obzir opću razinu dohotka u državi

[30] Vidi GDPR, Preambula, točka 150

[31] Prema članku 83. GDPR-a: *„Za nepoštovanje naredbe nadzornog tijela iz članka 58. stavka 2. u skladu sa stavkom 2. ovog članka mogu se izreći upravne novčane kazne u iznosu do 20 000 000 EUR, ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.".* Vidi GDPR, čl. 83. st. 6

članici te ekonomsko stanje osobe. Predviđena je i primjena mehanizma konzistentnosti radi promicanja konzistentne primjene upravnih novčanih kazni.[32] Države članice trebale bi utvrditi i trebaju li i do koje mjere primjenjivati upravne novčane kazne za državna tijela. Izricanje upravne novčane kazne ili upozorenja ne utječe na primjenu ovlasti nadzornih tijela ili drugih sankcija na temelju ove Uredbe. (GDPR, Preambula, točka 150) U svakom slučaju novčane kazne trebale bi biti učinkovite, proporcionalne i odvraćajuće. (GDPR, Preambula, točka 151).[33]

Umjesto zaključka

Donošenje samog GDPR-a prvenstevno predstavlja ključni pravni okvir kojim je Europska unija odlučila je zaštiti privatnost svojih građana i povećati kontrolu nad obradom osobnih podataka građana uz uvođenje zakonske obveze procjene učinka na zaštitu podataka. Također, ova Uredba postrožuje dodatno i obradu posebnih kategorija podataka u području "e-zdravstva" te se samim time uistinu očekuje potreba edukacije i usklađivanja s novom Uredbom. Prekršitelje će stizati zaslužene kazne koje će uistinu značajno popuniti proračune samih članica EU. Propisana je gornja granica sankcija i upravnih novčanih kazni te je prepušteno nacionalinim zakonodavstvima da reguliraju same sankecije, međutim ukoliko neka članica slučajno i odaberu mekšu politiku, Europska komisija zasigurno neće! Stoga je izbor za tvrtke i institucija koje žele nastaviti poslovati u skladu sa zakonom vrlo jednostavan. Ili će svoje poslovanje uskladiti sa zahtjevima GDPR-a, ili će platiti visoku kaznu i nakon naučene lekcije pokrenuti usklađivanje sa zahtjevima GDPR-a koji se od 25. svibnja 2018. počinje primjenjivati na području Europske unije.

Literatura

1. Adams S, Purtova N, Leenes R. Under Observation: The Interplay Between eHealth and Surveillance, Springer 2016.

[32] Primjerice, u pravnim sustavima Danske i Estonije nisu dopuštene upravne novčane kazne kako su navedene u ovoj Uredbi. Pravila za upravne novčane kazne mogu se primjenjivati na način da u Danskoj nadležni nacionalni sudovi izriču novčanu kaznu kao kaznenu sankciju, a da u Estoniji nadzorno tijelo izriče novčanu kaznu u okviru prekršajnog postupka, pod uvjetom da takva primjena pravilâ u tim državama članicama ima istovrijedni učinak kao i upravne novčane kazne koje izriču nadzorna tijela. Stoga bi nadležni nacionalni sudovi trebali uzeti u obzir preporuku nadzornog tijela koje ukaže na novčanu kaznu. U svakom slučaju novčane kazne trebale bi biti učinkovite, proporcionalne i odvraćajuće. Tako i šire vidi GDPR, Preambula, točka 151.

[33] Do prije nekoliko mjeseci vladalo je opće mišljenje da kazne neće biti rigorozne kako to Uredba propisuje, da će regulator biti blag te će prvo upozoriti prekršitelje što će se možda za one čiji će prekršaji biti maili možda uistinu i dogoditi. Međutim, Europska komisija je nedavno jasno dala do znanja da za ozbiljno kršenje Uredbe neće biti milosti. Kazna od 110 milijuna eura koju je Facebook dobio početkom ove godine propisana je direktno od strane Europske komisije. Iako na temelju potpuno druge regulative, ova kazna je propisana upravo zbog kršenje privatnosti građane i pružanja lažnih informacija o spajanju sa WhatsAppom. Tom je prilikom Facebook izjavio kako se osobni podaci korisničkih računa ne mogu spojiti, a dvije godine kasnije učinio je upravo to. Spojio je račune WhatsAppa sa računima Facebooka. Europska komisija reagirala je gotovo promptno i propisala kaznu od 110 milijuna eura; 0,5% ukupnih prihoda Facebooka na globalnoj razini i 50% maksimalne moguće koju propisuje regulativa o spajanju kompanija. Dakle, ako neka EU zemlja neće sama kazniti prekršitelja, a činjenica je da Hrvatska još nije ustanovila tijelo koje bi bilo odgovorno za provjeru kršenja i naplatu kazni, očito je da će to učiniti EU učiniti direktno. Samo nekoliko dana kasnije nakon prve presude, Italije je za isti prekršaj kaznila WhatsApp i time direktno popunila državni proračun za 3 milijuna eura.Vidi šire na portalu Damacija Danas, Kolumna Marije Boban, dostupno na https://www.dalmacijadanas.hr/konacno-zakon-na-strani-malog-covjeka-uskoro-cete-moci-zatraziti-brisanje-ili-uklanjanje-osobnih-podataka (30. 11. 2017.)

2. Blackmer WS. GDPR: Getting Ready for the New EU General Data Protection Regulation, Information Law Group, InfoLawGroup LLP, 2016, Retrieved 18. 11. 2017.
3. Boban M. Right to privacy and freedom of information in the modern information society. Proceedings of the Faculty of Law, Split. 2012.); 49(3):576-577.
4. Boban M. Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world, 16th International Scientific Conference on Economic and Social Development "The Legal Challenges of Modern World": Book of Proceedings/ Primorac Ž, Bussoli C, Recke N (ur.). Varaždin; Split; Koprivnica: Development and Entrepreneurship Agency; Faculty of Law; University North, Koprivnica, 2016, p. 191 – 202.
5. Boban M. ePrivacy and new European Data Protection Regime, // International Scientific Conference ESD 2016, Managerial Issues in Modern Business, Warsaw, Poland, 2016, p. 152-159.
6. Boban M. Upravljanje sigurnosnim rizicima i krizno upravljanje u mrežnoj komunikaciji "// Dani kriznog upravljanja 2014., Zagreb, str. 549-572
7. Boban M. "Krizno upravljanje i upravljanje sigurnošću informacijskih sustava kao temeljni oblici prevencije računalnog kriminaliteta" // 4th International Scientific and Professional Conference 'Police College Research Days in Zagreb, Zagreb, 2015, str. 27-52
8. Boban M. Kolumna, portal Dalmacija danas, 2017. https://www.dalmacijadanas.hr/konacno-zakon-na-strani-malog-covjeka-uskoro-cete-moci-zatraziti-brisanje-ili-uklanjanje-osobnih-podataka (30. 11. 2017.)
9. Castells M. The information age: economy, society and culture, Vol. I: The rise of the network society, Cambridge, Blackwell Publishers 1996.
10. Castells M. "Communication, Power and Counter-power in the Network Society". In: International Journal of Communication 2007; 1: 238-266.
11. Castells M. Communication power. Oxford/New York, Oxford University Press, 2009.
12. Charter of fundamental rights of the European Union (2010/C 83/02) EN 30.3.2010 Official Journal of the European Union C 83/389
13. Čizmić D, Boban M, Zlatović D. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilište u Splitu Pravni fakultet, Split, 2016.
14. DIRECTIVE (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
15. DIREKTIVA 95/46/EZ Europskog parlamenta i vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (OJ L 281, 23.11.1995, special edition in Croatian: Chapter 13 Volume 007 p. 88 – 107

16. European Commission - Press release, Brussels,18 May 2017, Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover, 2017. Dostupno na http://europa.eu/rapid/press-release_IP-17-1369_en.htm
17. Machlup F. Knowledge: its Creation, Distribution and Economic Significance, vol. III, The Economics of Information and Human Capital, Princeton, NJ, Princeton University Press 1984.
18. Mulgan G. Communication and Control: Networks and the New Organizations, Helsinki: Metaxis 1991.
19. 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, 4.5.2016).
20. Tuđman M. Uvod u informacijsku znanost, Zagreb: Školska knjiga 1993.
21. Tuđman, M. Teorija informacijske znanosti, Zagreb: Informator 1990.
22. Tuomi I. Corporate Knowledge: Theory and Practice of Intelligent, 1999.
23. Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12)