UČINAK NOVE EU UREDBE 2016/679 (GDPR) NA ZAŠTITU OSOBNIH PODATAKA U REPUBLICI HRVATSKOJ

*Prof. dr. sc. Jozo Čizmić**
*Doc. dr. sc. Marija Boban***

UDK 342.738::061.1EU
https://doi.org/10.30925/zpfsr.39.1.13
Ur.: 16. siječnja 2018.
Pr.: 19. veljače 2018.
Pregledni znanstveni rad

Sažetak

Nakon više od sedam 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 osobnih podataka 2016/679 ili GDPR (General Data Protection Regulation) zamjenjuje trenutnu EU direktivu i izravno se primjenjuje u svim državama članicama Europske unije. Mogućnost prilagodbe određenih dijelova ipak je ostavljena u nacionalnom zakonodavstvu zaključno s 25. svibnja 2018. kada se GDPR počinje primjenjivati! Ključna pretpostavka razvoja suvremene digitalne ekonomije temelji se na ubrzanom razvoju informacijskih i komunikacijskih tehnologija, istodobno stvarajući nove izazove i ugroze privatnosti i zaštite osobnih podataka. Obrada podataka, osobito obrada osobnih podataka, novi IT alati i digitalno tržište, razvilo je potrebu za povećanjem zaštite privatnosti novih digitalnih proizvoda i usluga. Rješenje je navedeno u novoj reformi EU okviru zaštite osobnih podataka koja unosi velike promjene u načine upravljanja osobnim podacima i izravno se primjenjuje na sve organizacije koje raspolažu osobnim podacima građana Europske unije. Također, GDPR sa sobom donosi bitne promjene u pravilima koja definiraju osobne podatke te uvoodi nove pojmove kao i usklađenost, planiranje, implementaciju, održavanje usklađenosti te procjenu učinka. U nekim slučajevima organizacije će trebati imenovati i kvalificiranog službenika za zaštitu osobnih podataka (DPO – Data Protection Officer) koji će odgovarati izravno Upravi. Ustanove i tvrtke dužne su usklađivanje završiti do 25. svibnja 2018., kada se GDPR počinje primjenjivati u cijeloj Europskoj uniji. U ovom radu autori će predstaviti odredbe i primjenu nove EU Uredbe o zaštiti podataka i odredbama javnog i privatnog sektora u provedbi GDPR-a, s posebnim naglaskom na procjenu učinka koja će osigurati modernizirani okvir za zaštitu podataka u Europi. Nova će pravila uspostaviti europski zakon o zaštiti podataka, uvodeći novu definiciju osobnih podataka i zamjenjujući trenutne nedosljedne nacionalne zakone u svrhu u povećanja razine zašite podataka kao i povećanja pravne sigurnosti u rastućoj digitalnoj ekonomiji.

Ključne riječi: *GDPR, osobni podaci, kazne, pseudonimizacija, pravo na zaborav, obrada podataka, službenik za zaštitu podataka, usklađenost, učinak, zaštita podataka*

1. UVOD

Tehnološkim razvojem i novim načinima obrade osobnih podataka, postalo je nužno donošenje novog instrumenta koji će osigurati zaštitu prava i temeljnih sloboda pojedinaca u vezi s obradom njihovih osobnih podataka. U svim modelima kroz povijest razvoja informacijske znanosti nedvojbena je činjenica da je informacija ključni fenomen, entitet, što se razmjenjuje u komunikacijskom procesu čija priroda nikada do kraja nije 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.[1] U suvremenom, informacijskom društvu informacije postaju temeljem procesa javnog informiranja, sastavnog dijela demokratskih i političkih procesa. Informacije postaju i važan element slobode i prava na širenje informacija koji u velikoj mjeri ovisi upravo o legitimnosti i mogućnosti upravljanja zbirkama podataka. Razvidno je da postupak širenja informacija, njihovog tiskanja, objavljivanja ili emitiranja u medijima podliježe njihovom pogrešnom interpretiranju. Logično, jedno od ustavnopravnih i diferencirajućih sredstava ograničavanja slobode javnog informiranja radi zaštite prava ličnosti jest pravo na ispravak informacije. Ustav Republike Hrvatske (Narodne novine, br. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14 – u daljnjem tekstu Ustav RH) jamči pravo na ispravak svakomu kome je javnom viješću povrijeđeno Ustavom i Zakonom utvrđeno pravo (Ustav RH, čl. 38.). Postupak širenja informacija, njihovog tiskanja, objavljivanja ili prikazivanja uređuje pravna regulativa javnog informiranja. U Republici Hrvatskoj informiranje se ostvaruje putem medija koji su podložni nacionalnom zakonodavstvu odnosno Zakonu o medijima ("Narodne novine", br. 59/04, 84/11, 81/13., dalje –ZM).

Ono što nije bilo sporno u postavkama informacijske znanosti jest činjenica da se pojava i razvoj informacijske znanosti povezuje sa: razmjenom znanja, komunikacijskim medijima te metodama i tehnikama obrade podataka. Ono što je

* Dr. sc. Jozo Čizmić, redoviti profesor Pravnog fakulteta Sveučilišta u Splitu; Jozo.Cizmic@pravst.hr.

** Dr. sc. Marija Boban, docentica Pravnog fakulteta Sveučilišta u Splitu; marija.boban@gmail.com.

1 Sa stajališta informacijske znanosti već od pedesetih 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.

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 i informacijskih procedura. [2] Nadalje, iako su i ranije postojale direktive[3] i zakonodavni i regulativni okvir zaštite osobnih podataka nova Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka 2016/679 (Opća uredba o zaštiti podataka – dalje GDPR) bitan je 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. Također, uvode se nove i pojednostavljuju se neke već postojeće definicije, određuju se 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.

2. ZAŠTITA OSOBNIH PODATAKA I NOVA OPĆA UREDBA O ZAŠTITI PODATAKA (GDPR)

Digitalizacija je okosnica razvoja informacijske superprometnice te otvara kompleksnost zaštite privatnosti i informacijske sigurnosti. Liberalizacija se ponajprije odnosi na otvorenost neograničenog komunikacijskog prostora s pratećim procesom kulturne globalizacije. Globalizacija pak, uz podršku informacijskih i komunikacijskih tehnologija i otvorena globalnog prostora, svjetske trendove premješta u lokalne okvire. 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.[4] Otvorenost arhitekture Interneta i njegov kontinuirani razvoj u kojemu su korisnici bili istovremeno i kreatori i pridonosili njegovu daljnjem razvoju, bile su njegove glavne snage razvoja.[5] Nezaustavljivi trend informacijskog društva unaprjeđuje kvalitetu komunikacija, oplemenjuje razvoj tehnologija, ali ima važan zadatak – uspostavljanje modela zaštite podataka, osobito zaštite osobnih podataka, najvrjednijeg dijela osobnosti i koncepta individualnosti i nasuprot globalnoj univerzalnosti jedan je od ključnih ciljeva reforme regulative zaštite podataka koja je

2 Tako i šire Boban, M., *Right to privacy and freedom of information in the modern information society,* Proceedings of the Faculty of Law, Split.,ol 49, br. 3., 2012., str. 576-577.

3 U ovom slučaju misli se poglavito na Direktivu 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) koja se donošenjem Uredbe 2016/679 stavlja izvan snage.

4 Usp. CASTELLS, M., *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press, 2001. str. 28-29.

5 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.

stupila na snagu 27. travnja 2016.[6] Nakon više od sedam 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 (engl. *General Data Protection Regulation* – dalje GDPR), unosi velike promjene u načine upravljanja osobnim podacima i izravno se primjenjuje na sve organizacije koje raspolažu osobnim podacima građana Europske unije. Nadalje, kao članica Europske unije, Hrvatska je obvezna uskladiti svoje zakonodavstvo s novodonesenom regulativom EU za područje zaštite podataka, kao i sve ostale države članice EU, do 2018. [7] Važnost 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 se cjelokupna pravna i sigurnosna zaštita dižu na višu razinu sigurnosti i zaštite u suvremenom informacijskom društvu.[8]

Uz navedenu Opću uredbu, sastavni dio usvojena 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 2016/680*. Tom će se Direktivom ujednačiti zaštita osobnih podataka koje obrađuju pravosudna i policijska tijela u državama članicama Europske unije.[9] Ona 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 njihovom obradom.[10]

Važno je istaknuti kako GDPR zamjenjuje Direktivu 95/46/EZ Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka te stupa na snagu danom donošenja i izravno se

6 Prije same Uredbe donesene su i smjernice o e-privatnosti kojima su stvoreni preduvjeti za zaštitu osobnosti u području elektroničkih komunikacija. Vidi detaljnije 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.

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

8 Detaljnije o Uredbi i sadržaju Uredbe te važnosti za zaštitu osobnih podataka vidi u: 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, str. 191– 202.

9 Za primjere paktične primjene GDPR-a vidi šire u VOIGT, P., BUSSCHE VON DEM, A., *The EU General Data Protection Regulation (GDPR): A Practical Guide,* Springer, 2017. Vidi i RUSTICI, C.*, Applying the GDPR: The Functional Specifications of Eu-Grade Privacy,* O'Reilly Media, 2017.

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

primjenjuje u svim državama članicama EU-a.

Direktiva 95/46/EZ	GDPR
• Identitet kontrolora • Svrhe obrade • Obaveza odgovoriti na subjekta podataka • Pravo pristupa, ispravaka i prigovora • Primatelji • Prijenos podataka	• Identitet kontrolora i DPO-a • Svrha • Razdoblje čuvanja podataka • Pravo pristupa, ispravaka, ograničenja i prigovora • Pravo na podnošenje žalbe • Primatelji • Prijenosi • Pravo povlaćenja suglasnosti u bilo kojem trenutku • Legitiman interes kontrolora ili treće osobe (ako je relevantno) • Informacije o profiliranju • Sve ostale informacije koje jamče zakonitost prerade

Tablica 1. Usporedba razlika između Direktive 95/46/EZ i nove Opće uredbe o zaštiti podataka (GDPR)[11]

Za nadzor će vjerojatno bti zadužena Agencija za zaštitu osobnih podataka (AZOP)[12] s mogućnošću izmjene naziva budući da je mogućnost prilagodbe određenih dijelova ipak ostavljena u nacionalnom zakonodavstvu zaključno s 25. svibnja 2018. kada se GDPR počinje primjenjivati.

11 Prilagođeno prema tekstu "Unpacking the European Commission General Data Protection Regulation - Getting into the Nitty Gritty of How to Comply", Baker McKenzie. Dostupno na https://m.acc.com/chapters/wash/.../BM-Unpacking-the-GDPR-FINAL-June-2017.ppt (10. 01. 2017.).

12 Agencija za zaštitu osobnih podataka je pravna osoba s javnim ovlastima, koja samostalno i neovisno obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o zaštiti osobnih podataka ("Narodne novine", broj 103/03, 118/06, 41/08, 130/11; 106/12 - pročišćeni tekst). Agencija je uspostavljena i djeluje samostalno i neovisno o izvršnoj i zakonodavnoj vlasti, ne primajući upute i naloge od bilo kojeg državnog tijela, kako je propisano Direktivom 95/46 Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka. Njezini glavni zadaci su učinkovito djelovanje na ispunjavanje svih prava i obaveza iz područja zaštite osobnih podataka, koje se Republici Hrvatskoj nameću kao punopravnoj članici Europske unije i Vijeća Europe, povećanje odgovornosti svih sudionika u procesu obrade osobnih podataka vezano za primjenu propisa koji su obuhvaćeni zakonskim okvirom zaštite osobnih podataka u Republici Hrvatskoj uz odgovarajuću primjenu mjera informacijske sigurnosti. Vidi više o Agenciji na: http://azop.hr/djelatnost-agencije (12. 01. 2018.) Također, kako GDPR stavlja van snage Direktivu, i uvodi Nadzorno tijelo, nužno je do svibnja 2018. donijeti i izmjene ZZOP-a i u pogledu definicije uloge same Agencije za zaštitu osobnih podataka te je uskladiti s Uredbom. U trenutku pisanja rada Zakon o primjeni GDPR-a je u postupku e-savjetovanja.

2.1. Nova definicija osobnog podatka prema GDPR-u

Nova EU Uredba donosi bitne promjene u pravilima koja definiraju osobne podatke i samu obradu podataka u cjelini. 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 je Uredba 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 izrijekom dopunu pravne definicijie prema kojem je osobni podatak svaki podatak kojim se "*osoba 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*;" (GDPR, čl. 4. st. 1.). Odnosno definicija izravno uvodi pojam *mrežni identifikator te se* nadalje u tekstu Uredbe po prvi put definiraju (i zakonski uređuju!) *genetski podac" i biometrijski podaci kao osobni podaci.* Naime*, genetski podaci* predstavljaju osobne podatke *"koji se odnose na nasljeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca;* (GDPR, čl. 4. st. 13.) dok se pod pojmom*. biometrijski podaci* podrazumijevaju se *"osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci".* (GDPR, čl. 4. st. 14.).

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 on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.* (GDPR, čl. 4. st. 11.). Novina je 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.

2.2. Teritorijalno područje primjene GDPR-a

Ključna izmjena u odnosu na raniju Direktivu i nacionalne zakone jest činjenica da se Uredba primjenjuje na obradu osobnih podataka koju obavlja voditelj obrade koji nema poslovni nastan u Uniji, već u mjestu gdje se pravo države članice primjenjuje na temelju međunarodnog javnog prava. (GDPR, čl. 3. st. 3.) Nadalje, Uredba se odnosi na obradu osobnih podataka u okviru aktivnosti poslovnog nastana voditelja

obrade ili izvršitelja obrade u Uniji, neovisno o tome obavlja li se obrada u Uniji ili ne. (GDPR, čl. 3. st. 1.) Odnosno, ova se Uredba primjenjuje na obradu osobnih podataka ispitanika u Uniji koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji, *ako su aktivnosti obrade povezane s: (a) nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje; ili (b) praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar Unije*. (GDPR, čl. 3. st. 2.) Veliki broj organizacija koje posluju na području Europske unije a bez poslovnog nastana u Europskoj uniji, započeo je proces usklađivanja s obzirom na visoke kazne koje Uredba propisuje. [13]

2.3. Uvjeti privole obrade podataka

Pretpostavka ispunjenja uvjeta obrade osobnih pdoataka jest činjenica da se obrada temelji na privoli odnosno voditelj obrade mora moći dokazati da je ispitanik dao privolu za obradu svojih osobnih podataka. (GDPR, čl. 7. st. 1.) U članku 7. st. 1. GDPR-a jasno je definirano kako "zahtjev za privolu mora biti predočen na način da ga se može jasno razlučiti od drugih pitanja, u razumljivom i lako dostupnom obliku uz uporabu jasnog i jednostavnog jezika čime se dokazuje da je osoba dala privolu u vidu pisane izjave koja se odnosi i na druga pitanja. Novost prema Uredbi jest da svaki dio takve izjave koji predstavlja kršenje ove Uredbe nije obvezujući. (GDPR čl. 7. st. 2.) Naime, osoba ima pravo u svakom trenutku povući svoju privolu te njeno povlačenje ne utječe na zakonitost obrade na temelju privole prije njezina povlačenja. Prije davanja privole, ispitanika se o tomu obavješćuje kao i o samom postupku povlačenja privole koji mora biti jednako jednostavan kao i njezino davanje. (GDPR, čl. 7. st. 3.) Uredba predviđa i postupak procjene dobrovoljnosti davanja privole kod kojeg se u najvećoj mogućoj mjeri uzima se u obzir je li, među ostalim, izvršenje ugovora, uključujući pružanje usluge, uvjetovano privolom za obradu osobnih podataka koja nije nužna za izvršenje tog ugovora. (GDPR, čl. 7. st. 4.)

2.4. Uvjeti koji se primjenjuju na privolu djeteta u odnosu na usluge informacijskog društva

Posebna su kategorija upravo osobni podaci djece gdje je ponajprije postavljena dobna granica 16 godina ali i mogućnost predviđanja niže dobne granice za davanje privole za obradu osobnih podataka djece i do 13 godina.[14] Države članice mogu u te svrhe zakonom predvidjeti nižu dobnu granicu, pod uvjetom da takva niža dobna

13 O usklađivanju europskog i američkog zakonodavstva u području zaštite podataka vidi u CALDER, A, *EU GDPR & EU-US Privacy Shield: A Pocket Guide,* IT Governance Ltd, 2017., str. 76-80.

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

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 mrežnom okruženju. Osobito je važan element "privole" – kada je osoba kao dijete dala privolu za obradu podataka, no nakon nekoliko godina je zatražila brisanje. Osoba ima opravdani razlog za brisanje podataka, jer kao dijete, tijekom davanja privole, nije mogla biti u potpunosti biti svjesna rizika koji su uključeni u proces obrade. [15] Ovo se osobito odnosi na društvene mreže i internetske forume.[16]

2.5. Pravo na brisanje ("pravo na zaborav")

Najvažniji iskorak 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 ako 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 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 ako osobni podaci više nisu potrebni u svrhu za koju su se prikupljali/koristili, kada ispitanik povuče suglasnost, kada se ispitanik protivi obradi i ne postoji legitiman razlog za nastavak obrade, ako 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[17] i/ili

15 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.*" (čl. 8. st. 3. GDPR).

16 Šire o tome vidi u RAGHENO, N. (dir.), Collectif, *Data Protection & Privacy: Le GDPR dans la pratique - De GDPR in de praktijk,* Anthemis, 2017.

17 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.*

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, u 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 voditelju obrade nalaže priopćivanje svakog ispravka ili brisanja osobnih podataka ili ograničenje obrade provedeno u skladu s člankom 16., 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 mrežnom 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*.

2.6. 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 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, primjerice selekcije, koju 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 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, i tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj. (Preambula, točka 25).[18]

Ovaj postupak do sada nije bio zakonski zahtjev i predstavlja iznimni trošak za velike organizacije a naročito može biti izazov, ako obrađujete osobne podatke online, na primjer na društvenim mrežama, forumima ili web stranicama. Organizacije u

Uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave. (čl. 16. GDPR).

18 Sukladno tekstu preambule Uredbe. Vidi GDPR, t. 25., str. 5.

javnom i privatnom sektoru moraju prema Uredbi udovoljiti tim zahtjevima inače ih očekuju velike kazne.

2.7. Službenik za zaštitu podataka

Kako bi se osigurala usklađenost organizacije potrebni su stručnjaci koji razumiju zahtjeve GDPR-a i koji su dobro obučeni za planiranje, implementaciju i održavanje usklađenosti imaju organizacije prema samoj Uredbi. Na tom tragu, stupanjem GDPR-a na snagu, mnoge tvrtke obvezu imenovanja kvalificiranog službenika za zaštitu podataka (engl. *Data Protection Officer* – DPO) koji će izravno odgovarati Upravi.[19] (GDPR, čl. 37.) Također, službenik za izvršavanje djelujeneovisno u izvršenju svojih obveza i odgovara izravno upravi kako je i izrečeno u čl. 38 GDPR-a.[20] Nadalje, grupa poduzetnika može imenovati jednog službenika za zaštitu podataka pod uvjetom da je službenik za zaštitu podataka lako dostupan iz svakoga 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, 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

19 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.

20 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.).

kao kontaktna točka za nadzorno tijelo vezano uz pitanje 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 svrhu obrade. (GDPR, čl. 39. st. 2.).

2.8. Kazne za povrede nacionalnih pravila i upravne sankcije

Donošenje GDPR-a ključni je pravni okvir kojim je Europska unija odlučila zaštititi privatnost svojih građana. Prekršitelje će stizati zaslužene kazne koje će uistinu bitno popuniti proračune samih članica EU. Ako neke 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. 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 za ljudska prava (Preambula, točka 149.).

Počevši s postroženim pravilima obrade, najvažniji je naglasak na kaznenim odredbama. Nepoštivanje odredbi Uredbe povlači kazne i to drakonske - do 4% ukupna godišnjeg prometa na svjetskoj razini ili do 20 milijuna eura, koja god vrijednost bude viša. Za razliku od ranije, odnosit će se na sve tvrtke koje posluju na području Europske unije (a ne samo one koje su registrirane u EU!). Europska komisija je također nedavno jasno dala do znanja da za ozbiljno kršenje Uredbe neće biti milosti. Kaznu od 110 milijuna eura, koju je poznata društvena mreža *Facebook* dobila početkom ove godine, propisala je izravno Europska komisija. Iako na temelju potpuno druge regulative, ova kazna je propisana upravo zbog kršenja privatnosti građana i pružanja lažnih informacija o spajanju s *WhatsAppom*. Tom je prilikom predstavništvo *Facebook-a* izjavilo kako se osobni podaci korisničkih računa ne mogu spojiti, a dvije godine kasnije učinio je upravo to. Spojio je račune *WhatsApp-a* s računima Facebooka. Europska komisija reagirala je gotovo promptno i propisala kaznu od 110 milijuna eura; 0,5% ukupnih prihoda *Facebook-a* na globalnoj razini i 50% maksimalne moguće koju propisuje regulativa o spajanju kompanija. Dakle, ako neka država članica EU-a 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 izravno učiniti EU. Samo nekoliko dana kasnije nakon prve presude, Italija je za isti prekršaj kaznila WhatsApp i time popunila državni proračun za tri milijuna eura.[21]

21 Vidi šire European Commission - Press release, Brussels,18 May 2017, Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover,

3. PROCJENA UČINKA NA ZAŠTITU PODATAKA

Novina u Općoj urebi o zaštiti podataka je i procjena učinka na zaštitu podataka koja je detaljno propisana u čl. 35 Uredbe. Naime, navodi se ako postoji vjerojatnost da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, 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 stavku 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 kojom se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način uvelike 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.[22] (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.).

Upravo ovo poglavlje izazvalo je najviše interesa organizacija budući da dosadašnji važeći Zakon o zaštiti osobnih podataka nije uvodio obvezu procjene rizika i sigurnosti zaštite 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 podliježe voditelj obrade, ako su tim pravom uređuju posebni postupci obrade ili skupina dotičnih postupaka te je procjena učinka na zaštitu podataka već provedena

dostupno na: http://europa.eu/rapid/press-release_IP-17-1369_en.htm (20. 12. 2017.).

22 Prije usvajanja popisa iz stavaka 4. i 5. čl. 35. GDPR-a, nadležno nadzorno tijelo primjenjuje mehanizam dosljednosti 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.

kao dio opće procjene učinka u kontekstu donošenja pravne osnove, stavci od 1. do 7. članka 35. GDPR-a ne primjenjuju se osim ako države članice smatraju da je potrebno provesti takvu procjenu prije aktivnosti obrade.

3.1. Donošenje mjera za rješavanje problema rizika: zaštitne mjere, sigurnosne mjere i mehanizmi za osiguravanje zaštite osobnih podataka

Već je Direktivom 95/46/EZ predviđena opća obveza izvješćivanja nadzornih tijela o obradi osobnih podataka. Nametanjem te obveze stvarao se administrativni i financijski teret, a ona nije u svim slučajevima dovela do poboljšanja zaštite osobnih podataka. Uredba stoga nastoji ukinuti takve sveobuhvatne obveze općeg obavješćivanja i zamijeniti ih djelotvornim postupcima i mehanizmima koji se umjesto toga usredotočuju na one vrste postupaka obrade koji vjerojatno mogu prouzročiti visok rizik za prava i slobode pojedinaca zbog svoje prirode, opsega, konteksta i svrha. Takve vrste postupaka obrade mogu biti osobito one koje uključuju upotrebu novih tehnologija ili one koje su nove vrste i s obzirom na koje voditelj obrade još nije proveo procjenu učinka na zaštitu podataka ili za koje je procjena učinka na zaštitu podataka postala potrebna s obzirom na vrijeme koje je proteklo od prvotne obrade.[23] Nadalje, u takvim slučajevima, 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. 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.[24]

Kao jedan od temeljnih aspekata sigurnosti i zaštite podataka i informacijskih sustava općenito je važno istaknuti kriptografiju kao znanost o prikrivanju informacijskih sadržaja i onemogućavanju njihova razumijevanja, modificiranja i uporabe neovlaštenih (neautoriziranih) subjekata.[25] Ona se temelji na matematičkim tehnikama koje su povezane sa sigurnosti informacija na način da se ponajprije vrši provjera *vjerodostojnosti, tajnosti, provjera podrijetla informacije i identiteta korisnika, te dokazivanje odgovornosti korisnika za određenu radnju* koji su ujedno i najvažniji aspekt pri uspostavljanju sustava zaštite podataka općenito odnosno u ovom slučaju zaštite osobnih podataka.[26]. Pojmovno definicija glasi:

Vjerodostojnost (engl. *Data integrity*) - brine o tomu da ne dođe do neovlaštene promjene informacije, kao što su ubacivanje informacije, brisanje informacije i zamjena informacije. Da bi se osigurala vjerodostojnost, mora postojati način provjere

23 Vidi GDPR, Preambula, točka 89.
24 Prema GDPR, Preambula, točka 90.
25 Usp. PANIAN, Ž., *Kontrola i revizija informacijskih sustava*, Sinergija, Zagreb, 2001., str. 107
26 O tome šire vidi u GERTZ, M., GULDENTOPS, E., STROUS, L., (ed.), *Integrity, internal control and security in information systems: connecting governance and technology,* IFIP TC11/WG11.5 Fourth Working Conference on Integrity and Internal Control in Information Systems, November 15-16, 2001, Brussels, Belgium, Springer, 2002., str. 3-10.

da li je informacija promijenjena od strane neovlaštene osobe.[27]

Tajnost (engl. *Confidentiality)* **-** osigurava da je sadržaj informacije dostupan samo onima koji su za to ovlašteni. Postoje brojni načini zaštite tajnosti, počev od fizičke zaštite do matematičkih algoritama koji sakrivaju podatke od neovlaštenih osoba.[28]

Provjera identiteta (engl. *Autentification)* - koristi se na razini korisnika i na razini informacije.[29] Dakle, autentifikacija je postupak utvrđivanja identiteta korisnika (osobe ili programa), a izvodi se prije nego se korisniku dopusti pristup resursima. Time se onemogućava neovlaštenim korisnicima korištenje sustava (ili dijelova sustava). Postupak autentifikacije se sastoji od dva dijela: identifikacije i potvrde. Identifikacija je proces gdje korisnik daje svoj identitet, dok je potvrda proces potvrđivanja danog identiteta.[30] Stoga ispravnost postupka autentifikacije najviše ovisi o upotrijebljenoj proceduri potvrde. Temeljni tipovi autentifikacije, korišteni u raspodijeljenim sustavima, su:

- prijava korisnika (engl. *user login authentication*) – bavi se potvrdom korisnika od sustava, u vrijeme prijave.
- jednosmjerna autentifikacija (engl. one-way authentication) – bavi se potvrdom identiteta jednog korisnika, od drugog korisnika.
- dvosmjerna autentifikacija (engl. *two-way authentication*) – bavi se obostranom autentifikacijom, gdje korisnici koji komuniciraju, potvrđuju jedan drugom svoj identitet.[31]

Nadalje, nužno je pojasniti i tri osnovna autentifikacijska pristupa:

1. *dokaz znanjem* (engl. *proof by knowledge*) – u ovom pristupu, autentifikacija sadržava potvrdu nečega što zna samo autorizirani korisnik. Primjer je autentifikacija lozinkom (password). Ovaj pristup sadrži dva tipa autentifikacije: direktnu metodu (engl. *direct demonstration method*) i metodu izazov-odgovor (engl. *challenge–response method*). U direktnoj metodi korisnik potvrđuje svoj identitet dajući određenu informaciju (lozinku) koju sustav uspoređuje s ranije pohranjenom. Druga metoda funkcionira na način, da korisnik točno odgovara na pitanje (engl. challenge)

27 O važnosti vjerodostojnosti podataka vidi GOLDENBERG, B. J., *CRM in Real Time: Empowering Customer Relationships*, Information Today, Inc., 2008., str. 101.

28 Vidi CHUNG, Y., YUNG, M., *Information Security Application,* 11th International Workshop, WISA 2010, Jeju Island, Korea, August 24-26, 2010, Revised Selected Papers, Springer, 2011., str. 7.

29 Dva korisnika koja počinju komunikaciju se trebaju predstaviti jedan drugome. Prije početka rada većine operacijskih sustava, zahtjeva se predstavljanje korisnika, da bi se mogao odrediti dopušteni sigurnosnu razinu rada. Predstavljanje na razini informacije znači da za informaciju koja prolazi komunikacijskim kanalom treba provjeriti odakle dolazi, tko je vlasnik informacije, kojeg datuma je stigla, kojeg je tipa, koliko je stara itd. Šire o tome YORAV, K. (Ed.), *Hardware and software, verification and testing,* Third International Haifa Verification Conference, HVC 2007, Haifa, Israel, October 23-25, 2007 : proceedings, Springer, 2008., str. 148.

30 Tako i šire PINTELON, R., SCHOUKENS, J., *System identification: a frequency domain approach*, John Wiley and Sons, 2001., str. 17-19.

31 Vidi WRYCZA, S., *Systems Analysis and Design for Advanced Modeling Methods: Best Practices*, IGI Global snippet, 2009., str. 130.

koje postavlja sustav.[32]

2. *dokaz posjedovanjem* (engl. *proof by possession*) – svoj identitet korisnik dokazuje predočenjem predmeta koji može posjedovati samo autorizirani korisnik. Primjer takvog predmeta je plastična kartica s magnetskom trakom na kojoj su upisani bitni podaci u električnom obliku.
3. *dokaz osobinom* (engl. *proof by property*) – identitet se dokazuje provjerom nekih fizičkih osobina korisnika koje nije lako krivotvoriti. Mjerena osobina mora biti jedinstvena za svakog korisnika. Neke od ovih osobina su: otisak prsta, glas, potpis, mrežnica oka. [33]

Od ova tri predočena pristupa autentifikaciji, dokaz znanjem i dokaz posjedovanjem, mogu se upotrijebiti za sve tipove autentifikacije u sigurnim raspodijeljenim sustavima, dok je dokaz osobinom općenito ograničen na autentifikaciju ljudi, u sustavima opremljenim posebnim instrumentima.[34] Vrlo važan aspekt u ovom postupku jest i *nemogućnost izbjegavanja odgovornosti (*engl. *Non-repudiation)* Predstavlja temelj gore navedenih postavki i omogućava povezivanje vjerodostojnosti, tajnosti i identifikacije na način da osoba koja je autentificirana ujedno i snosi odgovornost za proces koji je izvršen.[35]

3.2. Mjere za rješavanje problema rizika zaštite podataka i upravljanje sigurnosnim rizicima

Sigurnost kod procjene učinka zaštite podataka najveći je izazov za upravu svake organizacije koja suočena s rizicima zaštite podataka pronalazi strategije za rješavanje istih prema načelu minimaliziranja sigurnosnih rizika. Općenito, rizik se definira kao opasnost da neka poduzeta aktivnost dovede do neželjenih posljedica, dok sigurnosni informacijski rizik definiramo kao opasnost da primjena informacijske tehnologije dovede do neželjenih posljedica u poduzeću i/ili njegovoj okolini. Budući da su rizici sastavni dio procesa poslovanja treba nastojati razviti i provesti primjereni skup postupaka odnosno metodologiju upravljanja rizicima.[36] Kao i svaki upravljački

32 Šire u BRANDS, S. A., *Rethinking public key infrastructures and digital certificates: building in privacy*, MIT Press, 2000., str. 192.

33 O upotrebi autentfikacijskih sustava u praksi putem dokaza posjedovanjem odnosno karakteristikama – putem otiska prsta, oblika lica ili zjenice oka odnosno o biometriji u praksi elektroničkog poslovanja vidi u NANAVATI, S., THIEME, M., NANAVATI, R., *Biometrics: identity verification in a networked worl*", John Wiley & Sons, 2002., str. 191.

34 O primjerima pouzdanog autentifikacijskog protokola vidi šire u TUNG, B., *Kerberos: a network authentication system*, Addison-Wesley, 1999., str. 93. Vidi i GARMAN, J., *Kerberos: the definitive guide*, O'Reilly Media, Inc., 2003., str. 6-7.

35 Kao primjer može se promatrati proces podizanja elektroničkog novca iz banke. Nakon što je potrošio sav novac, neodgovorni korisnik može tvrditi da on nije obavio tu radnju i poželi povrat novca na svoj račun od banke. Banka u tom slučaju mora imati mehanizam dokazivanja da je upravo taj korisnik odgovoran za tu radnju. Razriješenje situacije se najčešće postiže korištenjem nezavisnog posrednika kojem svi vjeruju (engl. *trusted party*). O tome vidi PAVLOV, A., NATHAN VAN DE WOUW, N. VAN DE W., NIJMEIJER, H., *Uniform output regulation of nonlinear systems: a convergent dynamics approach*, Springer, 2006., str. 146.

36 O upravljanju sigurnosnim rizicima vidi BOBAN, M., *Upravljanje sigurnosnim rizicima i*

proces, i proces upravljanja rizicima treba pomno planirati. Takvim bi planom trebale biti obuhvaćene sljedeće aktivnosti:

- identifikacija rizika,
- ispitivanje vjerojatnosti i kvantifikacija rizika,
- utvrđivanje prioriteta rizika,
- identifikacija protumjera,
- utvrđivanje odnosa troškova i koristi od primjene protumjera,
- izbor najdjelotvornijih protumjera,
- implementacija izabranih protumjera,
- definiranje mjera otklanjanja možebitnih šteta, te
- nadzor, revizija i modifikacija plana i postupaka. [37]:

Sigurnosna informacijska politika temelj je sigurnosna sustava tvrtke. U praksi se prevodi u skup organizacijskih pravila i postupaka koji u svojoj ukupnosti čine normativni okvir sigurnosne politike koju provodi menadžment danog poduzeća.[38] Najvažnija karakteristika sigurnosne politike poduzeća jest da mora biti formalizirana odnosno sigurnosne mjere koje se provode na razini poduzeća moraju biti formalizirane a sigurnosna politika mora poprimiti karakter službenog dokumenta obvezujućeg za sve djelatnike poduzeća. U razvoju sigurnosne politike na razini menadžmenta poduzeća sudjeluju svi djelatnici poduzeća s naglaskom na tehničko osoblje i srednji menadžment budući da tehničko osoblje najbolje poznaje mogućnosti pojave određenih problema praktične naravi dok srednji menadžment ima ovlasti i snagu da prihvaćenu politiku provede u djelo.[39]

Već pri samom stvaranju sigurnosne politike valja razmišljati o mogućnostima njezine implementacije što podrazumijeva poznavanje razine odgovornosti za svakog djelatnika te odgovornost svakog pojedinca da ukaže na eventualnu nemogućnost provođenja te politike budući da sigurnosna politika koja se ne može provesti može značiti praktično njezino nepostojanje.

- Dakle, uz samo poznavanje stupnja odgovornosti pri provođenju djelatnici su dužni i izvršavati određene procedure definirane sigurnosnom politikom poduzeća. Razlikujemo tri skupine takvih procedura:
- procedure za prevenciju sigurnosnih problema,
- procedure za prepoznavanje nedopuštenih aktivnosti i
- komunikacijske procedure.[40]

Procedure za prevenciju sigurnosnih problema u taktičkom smislu ne definiraju

krizno upravljanje u mrežnoj komunikaciji, Dani kriznog upravljanja 2014., Zagreb, 2014., str. 549-572.

37 Šire u PANIAN, Ž., "*Izazovi elektroničkog poslovanja*", Narodne novine, Zagreb, Ožujak 2002., str. 55.

38 O ulozi sigurnosne politike u informacijskoj sigurnosti vidi GHONAIMY, M. A. R., EL-HADIDI, M. T., ASLAN, H. K., *Security in the information society: visions and perspectives*, IFIP TC11 17th International Conference on Information Security (SEC2002), May 7-9, 2002, Cairo, Egypt, Springer, 2002., str. 198.

39 O organizacijskoj zaštiti vidi šire u ŠIMOVIĆ, V., ŠIMUNDIĆ, S., BAČA, M., *Policija i informatika*, Ministarstvo unutarnjih poslova, Zagreb, 1998., str. 73.

40 Vidi PANIAN Ž., op. cit., Izazovi..., str. 57. Vidi i BERINATO, S., *Reinvention in progress*, CSO, sv. 5, br. 5, ISSN 1540-904X, CXO Media Inc., svibanj 2006., str. 36-38.

kako će se provoditi određene sigurnosne procedure već što je cilj provođenja tih procedure i tko će preuzeti obvezu njihovog izvršavanja. Način njihovog provođenja određuje se na temelju analizom rizika kojima sustav može biti izložen i eventualnih nedostataka promatranog sustava.

Procedure za prepoznavanje nedopuštenih aktivnosti obuhvaća nekoliko jednostavnih procedura koje izvršava administrator sigurnosti ili pak odgovarajući računalni program. Temeljni način otkrivanja pokušaja «nedopuštenih aktivnosti» odnosno najčešće neovlaštena pristupa informacijskim sustavima jest nadzor nad prijavljivanjem sustavu na način da se prijave korisnika bilježe u odgovarajućim datotekama, a programi analiziraju koliko je bilo neuspjelih pokušaja, kada su izvršeni, koliko učestalo, u kojem dijelu poduzeća i sl. Također, najvažnije je da ovaj nadzor mora biti trajan kako bi se moglo pravovemeno reagirati.

Komunikacijske procedure definiran su način komunikacije između korisnika i administratora sigurnosti informacija što uvjetuje djelotvornost i učinkovitost sigurnosne politike poduzeća. Način rješavanja manjih problema može biti neformalan, ali prijave ozbiljnijih problema moraju biti dokumentirane u pisanom obliku u tu svrhu prilagođenim odgovarajućim obrascima (prijava kvara, zahtjev za zamjenu lozinke i slično).

U procesu elektroničke komunikacije nakon međusobnog utvrđivanja identiteta, partneri u komunikaciji počinju razmjenjivati razne poruke. Međutim, nije zajamčeno da sve poruke dolaze baš od onoga korisnika koji tvrdi da poruke šalje. Netko se, naime, može krivo predstaviti te time doći do podataka koji mu ne pripadaju. Rješenje se nalazi u autentifikaciji pojedinih poruka korištenjem digitalnog potpisa. .[41]

Prilikom planiranja i kreiranja sigurnosne politike poduzeća nužno je istaknuti usklađenost elemenata sigurnosnih procedura sa zakonskim i drugim odredbama i propisima te s ugovornim odredbama s drugim pravnim i fizičkim osobama. Pod navedenim podrazumijeva se poštivanje općih načela zakonitosti, kaznenog i građanskog prava, podzakonskih propisa, ugovornih obveza, unutarnjih pravila u poduzeću te uvriježenih poslovnih običaja i uzanci. Između ostalog, nužnost predstavlja i poštivanje uobičajenih etičkih normi koje nisu formalno propisane a tiču se primjerice privatnosti pojedinca.[42] Dakle, u određenoj mjeri trebalo bi sankcionirati

41 Digitalni potpis je u osnovi jedan veliki broj koji ovisi o poruci koja se potpisuje. Njegova su svojstva kako slijedi: primatelj može potvrditi identitet za koji se izdaje pošiljatelj, pošiljatelj ne može kasnije negirati sadržaj potpisane poruke te primatelj ne može nikako sam mijenjati potpisanu poruku. Prvo svojstvo je, primjerice, potrebno u financijskim sustavima. Kada računalo klijenta naruči od računala banke kupnju tone zlata, računalo banke mora biti sigurno da računalo koje naručuje kupnju zaista pripada kompaniji čiji se račun u transakciji tereti. Drugo se svojstvo koristi za zaštitu banke od prijevare. Ako bi banka kupila tonu zlata, a odmah nakon toga cijena zlata naglo padne, neka bi korisnik mogao tužiti banku da nikada nije naručila tu kupovinu. Kad banka priloži potpisanu poruku, klijent mora povući tužbu. Treće svojstvo služi za zaštitu klijenta u slučaju naglog porasta cijene zlata kad bi banka pokušala reći da je mušterija naručila jednu šipku umjesto tone zlata. O tome vidi MILLER, F.P, VANDOME, A. M., MCBREWSTER, J., *Digital Signature: Electronic Signature, Public- Key Cryptography, Signature, E-Mail, Contract, Cryptographic Protocol*, Bit Array, Global Trust Center, Cryptography, Alphascript Publishing, 2010., str. 55.

42 O usklađenosti etičkih normi i sigurnosne politike vidi u IACOVINI, J., *The human side*

informacijski sadržaj koji se tiče bilo prenošenja prijetećih, lažnih i podrugljivih informacija koji mogu remetiti odnose među zaposlenima, širiti rasnu, nacionalnu ili vjersku netrpeljivost, te ugrožavati privatnost pojedinca. Glavni problem upravo je uspostavljanje mjerila evaluacije i kontrole što se može riješiti postavljanjem etičkog povjerenstva čiji zadatak bi bio utvrđivanje etičkih normi unutar poduzeća, prevencija krštenja prava zaposlenih i eventualno sankcioniranje kršenja postavljenih normi.

3.3. Mehanizmi za osiguravanje zaštite osobnih podataka

Sigurnost infrastrukture javnog ključa kao elementa sigurnosne politike prilikom provedbe i općenito nadmašuje zahtjeve tipičnog sigurnosnog sustava za obradu transakcija. Naime, izdavanje samo jednoga pogrešnog certifikata te sama penetracija neovlaštenog korisnika u sustav certifikacijskog autoriteta može rezultirati neograničeno velikim brojem loših transakcija ili izdavanjem mase nevjerodostojnih certifikata.[43]

Osnovni zahtjev sigurnosne politike javnog ključa odnosno certifikacijskog ključa koji podržava poslovanje kritične aplikacije jest činjenica da mora koristiti hardverske kriptografske module za potpisivanje certifikata, jer je softverski zasnovana kriptografija previše podložna probojima i zlouporabama. Ključevi kojima se povezuje veći broj certifikacijskih autoriteta, tzv. korijenski ključevi (engl. *Root-key*).[44], općenito su dužeg vijeka, pa zahtijevaju posebne mjere opreza, među koje spada pohranjivanje privatnog ključa u sigurnim, *offline* hardverskim jedinicama. Pojedini dijelovi takvih ključeva moraju biti poznati većem broju ovlaštenih osoba, od kojih svaka zna samo svoj dio ključa i koje moraju zajednički potpisivati certifikate u kontroliranom procesu. Također, valja primjenjivati i dodatne elemente sigurnosne politike kako slijedi:

- *fizičko osiguranje materijalnih resursa* (prostorija, zgrada i opreme u kojima je smješten certifikacijski autoritet)
- *kadrovske sigurnosne mjere* (kontrola aktivnosti svih osoba koje imaju pristup certifikacijskom autoritetu i njihova posebna edukacija) i
- *proceduralne kontrole* (definiranje precizne sigurnosne politike i obvezna dvostruka kontrola nad osjetljivim funkcijama). [45]

S obzirom na to da sigurnost certifikacijskih autoriteta mora biti iznimno visoka sama ulaganja u izgradnju i troškovi funkcioniranja sigurnih resursa su takvi da ih mnoga poduzeća za sebe ne mogu pokrivati. Unajmljivanje odnosno *outsourcing funkcija* certifikacijskog autoriteta ne mora uvijek biti najbolje rješenje jer poduzeća nerijetko žele kontrolu nad infrastrukturom javnog ključa: tko dobiva certifikat,

of organization change, Training & Development, 47(1), str. 65–68. Vidi i QUIGLEY, M., *Encyclopedia of information ethics and security*, Idea Group Inc (IGI), 2008., str. 321–322.

43 Vidi šire 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.

44 Vidi BUBAK, M., Computational science-- ICCS 2004: 4th International conference, Kraków, Poland, June 6-9, 2004: proceedings, LINK (Online service), Springer, 2004., str. 607.

45 Tako i PANIAN, Ž., op. cit., Izazovi elektroničkog poslovanja, str. 422.

koji je sadržaj certifikata te kako i kada se certifikati mogu ili moraju opozvati, ali i u rutinsko, svakodnevno funkcioniranje certifikacijskog autoriteta. Ipak, postoje rješenja koja pomiruju naizgled suprotstavljene potrebe u obliku *distribuirane funkcionalnosti*. Pod distribuiranom funkcionalnošću podrazumijeva se podjela funkcije infrastrukture poduzeća s globalnim certifikacijskim autoritetom. Poduzeća nadziru rad certifikacijskog autoriteta i kontinuirano administriraju i prate njegove aktivnosti. S druge strane, svakodnevne *pozadinske funkcije sigurne obrade podataka*, kao što je primjerice izdavanje certifikata uz uporabu kriptografskog hardvera i sigurno pohranjivanje podataka iz certifikata, delegiraju se globalnom certifikacijskom autoritetu. Nakon uspješne autentifikacije korisnika ili procesa, sustav mora pronaći način kako ograničiti pristup onim resursima za koje nemaju pristup. Taj zadatak sustav rješava korištenjem mehanizama kontrole pristupa. U osnovi su ti mehanizmi jednaki i za distribuirane i centralizirane sustave. Glavna razlika je u tome da su resursi u centraliziranom sustavu lokalno smješteni, pa se kontrolu pristupa tim resursima može obavljati centralno, dok je u raspodijeljenoj klijent-poslužitelj okolini, svaki poslužitelj odgovoran za kontrolu pristupa vlastitim resursima.

Kad se govori o kontroli pristupa u računalnim sustavima obično se koriste sljedeći pojmovi:

- *Objekti* – objekt je entitet kojemu se mora kontrolirati pristup. Može biti apstraktan entitet (proces, datoteka, semafor) ili fizički entitet (procesor, memorijski segment, pisač). Svaki objekt ima jedinstveno ime kojim se razlikuje od svih drugih objekata u sustavu. Svakom se objektu pridjeljuje i tip koji određuje skup operacija koje se mogu obaviti na tome objektu.
- *Subjekti* – subjekt je aktivan entitet čiji se pristup objektima mora kontrolirati. Drugim riječima, to je entitet koji želi pristupiti objektima i na njima izvršiti operacije. Primjeri subjekata su procesi i korisnici. Treba primijetiti da su subjekti istovremeno i objekti jer i oni također moraju biti zaštićeni. Radi toga i oni, kao i objekti, imaju jedinstveno ime.
- *Pravila zaštite* – pravila zaštite definiraju moguće načine međusobnog djelovanja subjekata i objekata. To znači da ta pravila upravljaju pristupom subjekata objektima. Svakom se paru (subjekt, objekt) pridružuje pravo pristupa koji su podskup skupa svih prava pristupa koje subjekt može izvršiti na objektu.[46]

3.4. Prethodno savjetovanje

Voditelj obrade savjetuje se s nadzornim tijelom prije obrade ako se procjenom učinka na zaštitu podataka iz članka 35. pokazalo da bi, u slučaju da 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 kršila Uredba,

46 Detaljnije o autorizaciji putem weba vidi u: KIZZA, J. M., *A Guide to Computer Network Security*, Springer, 2008., str. 203. Vidi i ČIZMIĆ, D., BOBAN, M., ZLATOVIĆ, D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost,* Sveučilište u Splitu, Pravni fakultet, Split, 2016.

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.).

4. PRAVNA SREDSTVA

1. "Povreda osobnih podataka" znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani (GDPR, čl. 4. točka 12.). Ako se povreda osobnih podataka ne rješava na odgovarajući način i pravodobno, može prouzročiti fizičku, materijalnu ili nematerijalnu/neimovinsku štetu pojedincima, kao što su gubitak nadzora nad osobnim podacima ili ograničavanje njihovih prava, diskriminacija, krađa identiteta ili prijevara, financijski gubici, neovlašteni obrnuti postupak pseudonimizacije, šteta za ugled, gubitak povjerljivosti osobnih podataka zaštićenih poslovnom tajnom ili bilo koju drugu ekonomsku ili društvenu štetu za dotičnog pojedinca.[47]

Jedan od temeljnih ciljeva GDPR-a jest dodatno ojačati prava na zaštitu osobnih podataka, odnosno pružiti pojedincima veću kontrolu nad njihovim osobnim podacima.[48] Među ostalim, GDPR-om se jamči i pravo na učinkoviti pravni lijek i pošteno suđenje (Preambula, toč. 4.). Ključni organizacijski oblik predviđen GDPR-om radi zaštite pojedinaca s obzirom na obradu njihovih osobnih podataka predstavlja osnivanje nadzornih tijela u državama članicama, koja su ovlaštena obavljati svoje zadaće i izvršavati svoje ovlasti potpuno neovisno (Preambula, točka 117.). "Nadzorno tijelo" je neovisno tijelo javne vlasti koje je osnovala država članica u skladu s člankom 51. GDPR-a (GDPR, čl. 4. točka 21.). U skladu s važećim zakonodavstvom Europske unije svaka država članica mora uspostaviti neovisno nadzorno tijelo zaduženo za praćenje provedbe propisa o zaštititi osobnih podataka, a istu takvu obvezu propisuje i GDPR. To bi trebalo uključivati i rješavanje pritužbi koje je podnio ispitanik, provođenje istraga o primjeni GDPR-a i promicanje javne svijesti o rizicima, pravilima, zaštitnim mjerama i pravima u svezi s obradom osobnih podataka (Preambula, točka 122.). Kako bi se osiguralo dosljedno praćenje i provedba GDPR-a u cijeloj Uniji, nadzorna tijela trebala bi u svakoj državi članici imati iste zadaće i stvarne ovlasti, među ostalim i ovlasti za vođenje istrage, korektivne ovlasti i sankcije

47 Tako *Opća uredba o zaštiti osobnih podataka*, Središnji državni ured za razvoj digitalnog društva, dostupno na https://rdd.gov.hr/UserDocsImages//dokumenti//GDPR%20%20Op%C4%87a%20Uredba%20o%20za%C5%A1titi%20osobnih%20podataka.pdf (23. 12. 2017.).

48 Vidi, *Nova regulacija zaštite podataka*, Comping d.o.o., slide 8., dostupno na: http://www.comping.hr/easyedit/UserFiles/GDPR/gdpr-brosura-screen.pdf (23. 12. 2017.).

te ovlasti za davanje odobrenja, savjetodavne ovlasti, posebno u slučajevima pritužbi pojedinaca. Svaka pravno obvezujuća mjera nadzornog tijela trebala bi biti u pisanom obliku, biti jasna i jednoznačna, navoditi nadzorno tijelo koje je izdalo mjeru, datum izdavanja mjere, sadržavati potpis predsjednika ili člana nadzornog tijela kojeg je on ovlastio, navoditi razloge za tu mjeru i upućivati na pravo na učinkoviti pravni lijek. Time se ne bi trebali isključiti dodatni zahtjevi na temelju postupovnog prava države članice. Donošenje pravno obvezujuće odluke podrazumijeva da to može dovesti do sudskog preispitivanja u državi članici nadzornog tijela koje je donijelo određenu odluku. (Preambula, točka 129.).

U Republici Hrvatskoj kao nadzorno tijelo uspostavljena je (za sada) Agencija za zaštitu osobnih podataka (dalje – AZOP). AZOP je pravna osoba s javnim ovlastima, koja samostalno i neovisno obavlja poslove u okviru svoga djelokruga i nadležnosti. Uspostavljena je i djeluje samostalno i neovisno o izvršnoj i zakonodavnoj vlasti, ne primajući upute i naloge od bilo kojeg državnog tijela. Glavni zadaci AZOP-a učinkovito su djelovanje u ispunjavanju svih prava i obveza iz područja zaštite osobnih podataka koje se Republici Hrvatskoj nameću kao punopravnoj članici Europske unije i Vijeća Europe. O povredi prava na zaštitu osobnih podataka AZOP odlučuje rješenjem koje ima karakter upravnog akta (arg. Zakon o zaštiti osobnih podataka, Pročišćeni tekst, Narodne novine, br. 106/2012., dalje - ZZOP, članak 24. st. 3.).[49]

2. Ne dovodeći u pitanje druga upravna ili sudska pravna sredstva, svaki ispitanik ima pravo podnijeti pritužbu nadzornom tijelu, osobito u državi članici u kojoj ima uobičajeno boravište, u kojoj je njegovo radno mjesto ili mjesto navodnog kršenja, ako ispitanik smatra da obrada osobnih podataka koja se odnosi na njega krši odredbe GDPR-a (GDPR, čl. 77. st. 1.). Ako pritužbu podnese ispitanik koji nema boravište u toj državi članici, nadzorno tijelo kojem je takva pritužba podnesena također bi trebalo biti predmetno nadzorno tijelo (Preambula, točka 124.).[50] Kada se donese odluka o odbacivanju pritužbe ispitanika u cijelosti ili djelomično, tu bi odluku trebalo donijeti nadzorno tijelo kojemu je pritužba podnesena (Preambula, točka 125.). Nakon pritužbe trebalo bi provesti istragu, u onoj mjeri u kojoj je to u konkretnom slučaju prikladno (Preambula, točka 141.).

De lege lata, u Republici Hrvatskoj svatko tko bude smatrao da mu je povrijeđeno neko pravo zajamčeno GDPR-om moći će podnijeti pritužbu AZOP-u, koja bi o eventualnoj povredi prava zajamčenih GDPR-om trebala odlučiti rješenjem protiv kojega žalba nije dopuštena, ali se može pokrenuti upravni spor (arg. ZZOP, članak 24.).

3. Nadzorno tijelo kojem je podnesena pritužba (u našem pravu AZOP) trebalo bi u razumnom roku izvijestiti ispitanika o napretku i ishodu pritužbe. Ako slučaj zahtijeva dodatnu istragu ili koordinaciju s drugim nadzornim tijelom, ispitaniku bi

49 Usp. AZOP, *Djelatnost i unutarnje ustrojstvo agencije*, podatak na stranici: http://azop.hr/djelatnost-agencije (27. 12. 2017.).

50 "Predmetno nadzorno tijelo" je nadzorno tijelo koje je povezano s obradom osobnih podataka zato što: (a) voditelj obrade ili izvršitelj obrade ima poslovni nastan na državnom području države članice tog nadzornog tijela; (b) obrada bitno utječe ili je izgledno da će bitno utjecati na ispitanike koji borave u državi članici tog nadzornog tijela; ili (c) podnesena je pritužba tom nadzornom tijelu (GDPR, čl. 4. točka 12.).

trebalo dati privremene informacije. Nadzorno tijelo trebalo bi podnositelja pritužbe obavijestiti i o mogućnosti podnošenja pravnog lijeka protiv odluka nadzornog tijela (vidi GDPR, čl. 78.). Kako bi se olakšalo podnošenje pritužbi, svako nadzorno tijelo trebalo bi poduzeti mjere poput izrade i dostupnosti obrasca za podnošenje pritužbe koji se može ispuniti i elektroničkim putem, ne isključujući pri tome i ostala sredstva komunikacije (GDPR, čl. 77. st. 2. i Preambula, točka 141.).

Kada zaštita prava ispitanika zahtijeva žurnost u postupanju, a osobito ako postoji opasnost da bi se provedba prava ispitanika mogla narušiti u većoj mjeri, nadzorno tijelo trebalo bi imati mogućnost donijeti opravdane privremene mjere na svojem državnom području s utvrđenim razdobljem trajanja koje ne bi smijelo biti duže od tri mjeseca (Preambula, točka 137.).

Pored propisanih upravnih novčanih kazni[51] i mjera koje je ovlašteno propisivati nadzorno tijelo u skladu s GDPR-om,[52] radi učinkovite provedbe odredaba GDPR-a države članice trebale bi propisati (dodatne) sankcije za svaku povredu odredaba GDPR-a. 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 (Preambula, točka 148.).

4. Svaki bi ispitanik trebao imati pravo na učinkoviti pravni lijek u skladu s člankom 47. Povelje Europske unije o temeljnim pravima,[53] ako ispitanik smatra da su prekršena njegova prava iz ove Uredbe ili ako nadzorno tijelo ne postupi po pritužbi, djelomično ili u potpunosti odbaci ili odbije pritužbu ili ne djeluje kada je takvo djelovanje nužno radi zaštite prava ispitanika. Drugim riječima, odredbom čl 78. st. 1. i 2. GDPR-a propisano je da, ne dovodeći u pitanje nijedan drugi upravni ili

51 Upravne novčane kazne uređene su čl. 83. GDPR-a. "Ako pravnim sustavom države članice nisu predviđene upravne novčane kazne, ovaj se članak može primjenjivati na način da novčanu kaznu pokreće nadležno nadzorno tijelo, a izriču je nadležni nacionalni sudovi pritom osiguravajući da su ta pravna sredstva učinkovita i imaju istovrijedan učinak kao i upravne novčane kazne koje izriču nadzorna tijela. U svakom slučaju novčane kazne koje se izriču moraju biti učinkovite, proporcionalne i odvraćajuće. Te države članice najkasnije do 25. svibnja 2018. obavješćuju Komisiju o odredbama svojih zakona koje donesu u skladu s ovim stavkom te, bez odgode, o svim daljnjim izmjenama zakona ili izmjeni koja na njih utječe".

52 Upravne novčane kazne izriču se uz mjere ili umjesto mjera iz članka 58. stavka 2. točaka od (a) do (h) i članka 58. stavka 2. točke (j), ovisno o okolnostima svakoga pojedinog slučaja.

53 Vidi Povelja Europske unije o temeljnim pravima, 2007/C 303/01, članak 47., Pravo na djelotvoran pravni lijek i na pošteno suđenje:
"Svatko čija su prava i slobode zajamčeni pravom Unije povrijeđeni ima pravo na djelotvoran pravni lijek pred sudom, u skladu s uvjetima utvrđenima ovim člankom.
Svatko ima pravo da zakonom prethodno ustanovljeni neovisni i nepristrani sud pravično, javno i u razumnom roku ispita njegov slučaj. Svatko ima mogućnost biti savjetovan, branjen i zastupan.
Pravna pomoć osigurava se za osobe koje nemaju dostatna sredstva, u mjeri u kojoj je takva pomoć potrebna za osiguravanje učinkovitog pristupa pravosuđu".

izvansudski pravni lijek, svaka fizička ili pravna osoba ima pravo na učinkoviti pravni lijek protiv pravno obvezujuće odluke nekog nadzornog tijela koja se na nju odnosi. Odnosno, svaki ispitanik ima pravo na učinkoviti pravni lijek ako nadležno nadzorno tijelo ne riješi pritužbu ili ne izvijesti ispitanika u roku od tri mjeseca o napretku ili ishodu pritužbe podnesene na temelju članka 77. GDPR-a.

Navedeni postupci protiv nadzornog tijela vodit će se pred sudovima države članice u kojoj nadzorno tijelo ima poslovni nastan (GDPR, čl. 78. st. 3.). U Republici Hrvatskoj učinkoviti pravni lijek protiv odluka/rješenja AZOP-a, odnosno propuštanja pravovremenog rješavanja pritužbe ispitanika od strane AZOP-a, bit će tužba ispitanika kojom će se pokrenuti upravni spor pred upravnim sudom. Naime, u Republici Hrvatskoj upravni sudovi stvarno su nadležni, među ostalim, odlučivati i o tužbama protiv pojedinačnih odluka javnopravnih tijela, odnosno o tužbama zbog propuštanja donošenja pojedinačne odluke ili postupanja javnopravnog tijela u zakonom propisanom roku (Zakon o upravnim sporovima, Narodne novine, br. 20/10, 143/12, 152/14, 94/16, 29/17, dalje - ZUS, čl. 12. st. 1. točke 1. i 3.), u ovom slučaju AZOP-a. Za rješavanje u navedenim sporovima mjesno nadležan bit će upravni sud na području kojeg ispitanik ima prebivalište, odnosno boravište. Ako, pak, ispitanik ne bi imao ni prebivalište ni boravište u Republici Hrvatskoj, mjesno nadležan bit će upravni sud na području kojeg AZOP ima sjedište, odnosno Upravni sud u Zagrebu. Tužbu će ispitanik biti dužan podnijeti u roku od 30 dana od dana dostave rješenja AZOP-a kojom je odlučio o pritužbi ispitanika, odnosno ako AZOP ne riješi pritužbu ili ne izvijesti ispitanika u roku od tri mjeseca o napretku ili ishodu pritužbe podnesene na temelju članka 77. GDPR-a, tužbu će se sudu trebati podnijeti najranije osam dana nakon proteka propisanog roka od tri mjeseca (arg. ZUS, čl. 24.).

5. Europski građani i druge fizičke osobe, ispitanici na području EU-a, od početka primjene GDPR-a imat će na raspolaganju znatno širi raspon pravnih mjera/sredstava kojima će moći zaštititi svoja prava od postupanja voditelja zbirki i izvršitelja obrade, kao i pravo na naknadu štete zbog povreda prava od strane voditelja ili izvršitelja obrade.[54] Drugim riječima, ne dovodeći u pitanje nijedan dostupan upravni ili izvansudski pravni lijek, uključujući i pravo na podnošenje pritužbe nadzornom tijelu na temelju članka 77. GDPR-a, ispitanik će imati pravo na učinkoviti pravni lijek protiv voditelja obrade ili izvršitelja obrade ako bude smatrao da su mu oni obradom njegovih osobnih podataka protivno odredbama GDPR-a prekršili njegova prava zajamčena GDPR-om (GDPR, čl. 79. st. 1.).

Odredbom članka 79. stavka 2. GDPR-a propisana su pravila o sudbenosti na način da će se postupci protiv voditelja obrade ili izvršitelja obrade moći voditi pred sudovima države članice u kojoj voditelj obrade ili izvršitelj obrade imaju poslovni nastan. Takvi će se postupci moći voditi i pred sudovima države članice u kojoj ispitanik ima uobičajeno boravište, osim ako je voditelj obrade ili izvršitelj obrade tijelo javne vlasti neke države članice koje kod obrade podataka djeluje izvršavajući svoje javne ovlasti (GDPR, čl. 79. st. 2. i Preambula, točka 145.).[55] Nadalje se propisuje da svaka

54 Tako KATULIĆ, T., *Stiže Opća uredba o zaštiti podataka*, dostupno na: http://www.bug.hr/molex/general-data-protection-regulation/97346.aspx (23. 12. 2017.).

55 Ako su posebna pravila o nadležnosti sadržana u ovoj Uredbi, osobito u svezi s postupcima

osoba koja je pretrpjela materijalnu ili nematerijalnu štetu[56] zbog kršenja ove Uredbe ima pravo na naknadu od voditelja obrade ili izvršitelja obrade za pretrpljenu štetu. (GDPR, čl. 82. st. 1.)[57] Sudski postupak za ostvarivanje prava na naknadu štete vodit će se pred sudovima koji su nadležni prema pravu države članice prema pravilima iz članka 79. stavka 2. GDPR-a (arg. GDPR, čl. 82. st. 6.).

Ako bi pravila o sudbenosti ukazivala na nadležnost sudova Republike Hrvatske, pravo na naknadu štete koju su počinili voditelj(i) obrade ili izvršitelj(i) obrade, ispitanici će moći ostvariti pred sudom opće nadležnosti (arg. Zakon o zaštiti osobnih podataka, Pročišćeni tekst, Narodne novine, br. 106/2012., članak 26.), a stvarno nadležni bit će općinski sudovi. Stvarna nadležnost općinskih sudova u sporovima za naknadu štete može se izvesti i proizlazi i iz odredaba čl. 52. Zakona o parničnom postupku (Narodne novine, br. 53/91, 91/92, 58/93, 112/99, 88/01, 117/03, 88/05, 02/07, 84/08, 123/08, 57/11, 148/11, 25/13, 89/14, dalje – ZPP) o mjesnoj nadležnosti suda u Republici Hrvatskoj za suđenje u sporovima o izvanugovornoj odgovornosti za štetu (vidi i ZPP, čl. 27.). Za suđenje u navedenim sporovima mjesno nadležni će biti, osim suda općemjesne nadležnosti, odnosno općinskog suda na čijem području voditelj obrade ili izvršitelj obrade imaju prebivalište/sjedište ili boravište (ZPP, čl. 46.-48.), i općinski sud na čijem je području štetna radnja počinjena ili sud na čijem je području štetna posljedica nastupila (ZPP, čl. 52. st. 1.)

6. Svatko tko drugome prouzroči štetu dužan ju je naknaditi ako ne dokaže da je šteta nastala bez njegove krivnje (Zakon o obveznim odnosima, Narodne novine, br. 35/2005, 41/2008, 125/2011, 78/2015, dalje – ZOO, čl. 1045. st. 1.). Ispitanici bi trebali dobiti potpunu i učinkovitu naknadu za štetu koju su pretrpjeli. Pojam štete u ovim predmetima trebalo bi široko tumačiti s obzirom na sudsku praksu Europskog suda tako da se u potpunosti odražavaju ciljevi GDPR-a. Time se ne dovode u pitanje zahtjevi za naknadu štete koja proizlazi iz kršenja drugih pravila prava Unije ili prava države članice. Obrada osobnih podataka kojom se krše odredbe GDPR-a također uključuje i obradu kojom se krše delegirani i provedbeni akti doneseni u skladu s GDPR-om i pravom države članice kojima se razrađuju pravila GDPR-a (Preambula, točka 146.).

U tom smislu svaki voditelj obrade koji je uključen u obradu odgovoran je za štetu prouzročenu obradom kojom se krše odredbe GDPR-a, a izvršitelj obrade je odgovoran za štetu prouzročenu obradom samo ako nije poštovao obveze iz GDPR-a koje su posebno namijenjene izvršiteljima obrade ili je djelovao izvan zakonitih uputa voditelja obrade ili protivno njima, a odgovarat će sukladno općim propisima o

kojima se traži pravni lijek, među ostalim i naknada od voditelja obrade ili izvršitelja obrade, opća pravila o nadležnosti poput pravila iz Uredbe (EU) br. 1215/2012 Europskog parlamenta i Vijeća (13) ne bi smjela dovoditi u pitanje primjenu takvih posebnih pravila (Preambula, točka 147.).

56 Više o tome kod RADOLOVIĆ, A., *Pravo osobnosti u novom Zakonu o obveznim odnosima,* Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Vol. 27, br. 1, 2006., str. 129-170 .

57 Tako KOVAČEK, M., *Važne stvari koje morate znati o Zakonu o zaštiti osobnih podataka (General Data Privacy Regulation – GDPR),* dostupno na: https://hitkonferencijablog.com/2017/06/20/vazne-stvari-koje-morate-znati-o-zakonu-o-zastiti-osobnih-podataka-general-data-privacy-regulation-gdpr/ (28. 12. 2017.).

naknadi štete (ZZOP, čl. 26.). Voditelj obrade ili izvršitelj obrade može se izuzeti od navedene odgovornosti ako dokaže da nije ni na koji način odgovoran za događaj koji je prouzročio štetu (GDPR, čl. 82. st. 2. i 3.).

Ako je u istu obradu uključeno više od jednog voditelja obrade ili izvršitelja obrade ili su u istu obradu uključeni i voditelj obrade i izvršitelj obrade i ako su odgovorni za bilo kakvu štetu prouzročenu obradom, svaki voditelj obrade ili izvršitelj obrade smatrat će se odgovornim za cjelokupnu štetu kako bi se osigurala učinkovita naknada ispitaniku (GDPR, čl. 82. st. 4.). Drugim riječima, odredbom članka 82. stavka 4. GDPR-a propisana je solidarna odgovornost za štetu prozročenu obradom osobnih podataka kada je počine zajedno voditelj i izvršitelj obrade, odnosno više od jednog voditelja ili izvršitelja obrade. U hrvatskom pravu solidarna odgovornost za štetu predviđena je i uređena odredbom članka 1107. ZOO-a.

Svaki voditelj obrade ili izvršitelj obrade koji je platio punu naknadu, može naknadno pokrenuti postupak za regres protiv drugih voditelja obrade ili izvršitelja obrade uključenih u istu obradu (Preambula, točka 146.). Kada voditelj obrade ili izvršitelj obrade plati punu (cjelokupnu) odštetu (naknadu) za pretrpljenu štetu, taj voditelj obrade ili izvršitelj obrade ima pravo regresa, odnosno ima pravo zatražiti od drugih voditelja obrade ili izvršitelja obrade koji su uključeni u istu obradu dio odštete koji odgovara njihovu udjelu u odgovornosti za štetu (GDPR, čl. 82. st. 5.). Odnosno voditelj obrade ili izvršitelj obrade koji je platio cjelokupnu odštetu za pretrpljenu štetu, može, kao solidarni dužnik koji je isplatio više nego što iznosi njegov udio u šteti, zahtijevati od svakog od ostalih dužnika (voditelja i/ili izvršitelja obrade) da mu naknadi ono što je platio za njega (ZOO, čl. 1109.).

7. Ako ispitanik smatra da su prekršena njegova prava iz GDPR-a, treba imati pravo ovlastiti kao zastupnika neprofitno tijelo, organizaciju ili udruženje,[58] koje je pravilno osnovano u skladu s pravom države članice, u čijem se statutu navode ciljevi od javnog interesa i koje je aktivno u području zaštite prava i sloboda ispitanika s obzirom na zaštitu njegovih osobnih podataka, da nadzornom tijelu (AZOP-u) podnesu pritužbu u njegovo ime i da ostvaruju prava na pravne lijekove protiv nadzornog tijela, voditelja i izvršitelja obrade, u ime ispitanika te da mu pomognu i u njegovo ime ostvare pravo na naknadu štete koju su počinili voditelj obrade ili izvršitelj obrade

58 U Republici Hrvatskoj to bi, primjerice, bile i neprofitne udruge koje se bave aktivnostima od interesa za opće dobro te se u tom smislu zauzimaju za promicanje i zaštitu ljudskih prava, prava nacionalnih manjina, prava osoba s invaliditetom i djece s teškoćama u razvoju, starijih i nemoćnih, jednakosti i ravnopravnosti te mirotvorstvu i borbi protiv nasilja i diskriminacije, promicanju vrijednosti Domovinskog rata, zaštiti, brizi i izobrazbi djece i mladih te njihovu aktivnom sudjelovanju u društvu, prevenciji i borbi protiv svih oblika ovisnosti, razvoju demokratske političke kulture, zaštiti i promicanju prava manjinskih društvenih skupina, promicanju i razvoju volonterstva, socijalnim uslugama i humanitarnoj djelatnosti, poticanju i razvoju socijalnog poduzetništva, zaštiti prava potrošača, zaštiti okoliša i prirode i zaštiti i očuvanju kulturnih dobara, održivom razvoju, razvoju lokalne zajednice, međunarodnoj razvojnoj suradnji, zaštiti zdravlja, razvoju i promicanju znanosti, obrazovanja, cjeloživotnog učenja, kulture i umjetnosti, tehničke i informatičke kulture, sporta, dobrovoljnog vatrogastva, traganja i spašavanja te drugim aktivnostima koje se po svojoj prirodi, odnosno po posebnim propisima o financiranju javnih potreba u određenom području mogu smatrati djelovanjem od interesa za opće dobro (vidi Zakon o udrugama, "Narodne novine" broj 74/14, 70/17, čl. 32.).

ako je to predviđeno pravom države članice (GDPR, čl. 80.).

Država članica može predvidjeti da će takvo tijelo, organizacija ili udruženje imati pravo, neovisno o mandatu ispitanika, podnijeti u toj državi članici pritužbu nadzornom tijelu i učinkoviti pravni lijek protiv nadzornog tijela i voditelja, odnosno izvršitelja obrade ako ima razloga smatrati da je do kršenja prava ispitanika došlo zbog obrade osobnih podataka protivno odredbama GDPR-a. *A contrario*, može se zaključiti da navedenim tijelima, organizacijama ili udruženjima ne smijelo biti dopušteno tražiti naknadu štete u ime ispitanika neovisno o mandatu ispitanika (Preambula, točka 142.), odnosno bez njegova ovlaštenja.

8. GDPR sadrži i odredbe kojima se rješava problem istovremenog vođenja identičnih postupaka pred nadležnim sudovima različitih država članica. Ako nadležni sud države članice posjeduje informacije ili ima razloga vjerovati da je postupak koji vodi po svom predmetu spora i strankama (ispitaniku, voditelju i/ili izvršitelju obrade) u svezi s identičnim predmetom koji je u tijeku na sudu druge države članice, dužan je kontaktirati taj sud u drugoj državi članici kako bi potvrdio postojanje tog postupka, odnosno takvih povezanih postupaka (GDPR, čl. 81. st. 1.). Smatra se da su postupci povezani kada su međusobno tako tijesno u vezi da je opravdano njihovo zajedničko saslušanje i odlučivanje o njima kako bi se izbjegla opasnost od proturječnih presuda u odvojenim postupcima (Preambula, točka 144.). U takvom slučaju, svi nadležni sudovi osim suda pred kojim je prvo pokrenut postupak mogu suspendirati svoj postupak *(*engl. *may suspend its proceedings)*. Kada se, pak, vodi prvostupanjski postupak, svi sudovi osim suda pred kojim je prvo pokrenut postupak mogu također na zahtjev jedne od stranaka odbiti nadležnost (*decline jurisdiction*) ako je sud pred kojim je najprije pokrenut postupak nadležan za odlučivanje u predmetnom postupku i ako njegovo pravo dopušta spajanje predmeta (GDPR, čl. 81. t. 2. i 3.). Kada bi se takvi identični postupci pokrenuli pred više sudova u Republici Hrvatskoj, postupak bi nastavio voditi sud pred kojim je parnica počela teći najprije, a svi ostali sudovi dužni su odbaciti tužbu (ZPP, čl. 194.).

5. UMJESTO ZAKLJUČKA

Tehnološkim razvojem i novim načinima obrade osobnih podataka postalo je nužno donošenje novoga instrumenta koji će osigurati zaštitu prava i temeljnih sloboda pojedinaca u vezi s obradom njihovih osobnih podataka. Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnome kretanju takvih podataka (Opća uredba o zaštiti podataka) predstavlja bitan napredak u području zaštite osobnih podataka. Sam učinak Opće uredbe ponajprije se ogleda u činjenici da se njenim donošenjem osigurava ujednačeno i jednoobrazno postupanje nadzornih tijela za zaštitu osobnih podataka, što će dovesti do jednostavnije i jednake zaštite prava svih pojedinaca u Europskoj uniji. Također, uvode se nove definicije i pojednostavljuju se neke već postojeće, određuju se 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 tijela za zaštitu osobnih podataka. Najveća novost je

uvođenje obveze procjene učinka prema kojoj, sukladno članku 35. st. 1. GDPR-a ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije same obrade osobnih podataka, provodi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka. Pritom mora voditi računa kako se jedna procjena može odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike. Samim time procjena rizika i zašita osobnih podataka po prvi put imaju evidentan učinak provođenja u području zakonodavstva. Naravno, pri provođenju procjene učinka na zaštitu podataka voditelj obrade svakako traži savjet od službenika za zaštitu podataka, ako je on imenovan (GDPR, čl. 35. st. 2.).

Uz navedenu Opću uredbu sastavni je dio usvojenoga zakonodavnog paketa i Direktiva o zaštiti pojedinaca pri obradi osobnih podataka od nadležnih tijela u svrhe sprječavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnome 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 se Direktivom jasno se određuje nadzor neovisnoga tijela za zaštitu osobnih podataka nad obradom istih.

Digitalizacija predstavlja okosnicu razvoja informacijske superprometnice te otvara kompleksnost zaštite privatnosti i informacijske sigurnosti. Liberalizacija se pak prvenstveno odnosi na otvorenost neograničenoga komunikacijskog prostora s pratećim procesom kulturne globalizacije. Globalizacija uz podršku informacijskih i komunikacijskih tehnologija i otvorenoga globalnog prostora svjetske trendove premješta u lokalne okvire. Nezaustavljivi trend informacijskoga društva unaprjeđuje kvalitetu komunikacija, oplemenjuje razvoj tehnologija, ali ima važan zadatak – uspostavljanje modela zaštite podataka, osobito zaštite osobnih podataka, najvrjednijega dijela osobnosti i koncepta individualnosti nasuprot globalnoj univerzalnosti, kao jednog od ključnih ciljeva reforme regulative zaštite podataka koja je stupila na snagu 27. travnja 2016. godine. Cilj je determinirati granice i maksimalno zaštititi protok podataka s naglaskom na obradu osobnih podataka na području Europske unije u suvremenome informacijskom društvu. Iz navedenih činjenica proizlazi potreba temeljitoga istraživanja i analize zaštite podataka u Republici Hrvatskoj sa sigurnosnoga, I pravnoga aspekta. Nadalje, kao članica Europske unije Hrvatska je obvezna uskladiti svoje zakonodavstvo s novodonesenom regulativom EU-a u području zaštite podataka, kao i sve ostale članice EU-a, do 2018. godine. Stoga je i izrada ovog rada upravo na tragu osvješćivanja i pojašnjavanja novina i primjene u javnom i privatnom sektoru koje Uredba donosi, a koje još uvijek nemaju pravnu podlogu u Republici Hrvatskoj budući da je Nacrt izmjena i dopuna Zakona o zaštiti osobnih podataka još uvijek u postupku javne rasprave.

LITERATURA

1. AZOP, Djelatnost i unutarnje ustrojstvo agencije, dostupno na: http://azop.hr/djelatnost-agencije.
2. BAKER MCKENZIE, "Unpacking the European Commission General Data Protection Regulation- Getting into the Nitty Gritty of How to Comply", dostupno na: https://m.acc.com/chapters/wash/.../BM-Unpacking-the-GDPR-FINAL-June-2017.ppt, 2017.
3. BERINATO, S., "Reinvention in progress, CSO, Sv. 5, br. 5, ISSN 1540-904X, CXO Media Inc., svibanj 2006., str. 36 – 38.
4. BLACKMER, W.S., GDPR: Getting Ready for the New EU General Data Protection Regulation, Information Law Group, InfoLawGroup LLP, 2016.
5. 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, str. 191–202.
6. 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.
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., Upravljanje sigurnosnim rizicima i krizno upravljanje u mrežnoj komunikaciji, Dani kriznog upravljanja 2014., Zagreb, 2014., str. 549-572.
9. BOBAN, M., Konačno zakon za strani malog čovjeka: uskoro ćete moći zatražiti brisanje ili uklanjanje osobnih podataka, kolumna na portalu Dalmacija danas, 2017, dostupno na https://www.dalmacijadanas.hr/konacno-zakon-na-strani-malog-covjeka-uskoro-cete-moci-zatraziti-brisanje-ili-uklanjanje-osobnih-podataka.
10. 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); str. 576-577, 2012.
11. BRANDS, S. A., Rethinking public key infrastructures and digital certificates: building in privacy, MIT Press, 2000.
12. BUBAK, M., Computational science, ICCS 2004, 4th International conference, Kraków, Poland, June 6-9, 2004, Proceedings, LINK (Online service), Springer, 2004., str. 607.
13. CALDER, A, EU GDPR & EU-US Privacy Shield: A Pocket Guide, IT Governance Ltd, 2017.
14. CASTELLS, M., Communication, Power and Counter-power in the Network Society, International Journal of Communication Vol 1, 2007, 2007., str. 238-266.
15. Castells, M., Communication power. Oxford/New York, Oxford University Press, 2009.
16. CASTELLS, M., The information age: economy, society and culture, Vol. I: The rise of the network society, Cambridge, Blackwell Publishers, 1996.
17. 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.
18. CHUNG, Y., YUNG, M., Information Security Applications, 11th International Workshop, WISA 2010, Jeju Island, Korea, August 24-26, 2010, Revised Selected Papers, Springer, 2011.
19. ČIZMIĆ, D., BOBAN, M., ZLATOVIĆ, D., Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilište u Splitu Pravni fakultet, Split, 2016.
20. 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.

21. 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.
22. 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.
23. GERTZ, M., GULDENTOPS, E., STROUS, L., (ed.)., Integrity, internal control and security in information systems: connecting governance and technology, IFIP TC11/ WG11.5 Fourth Working Conference on Integrity and Internal Control in Information Systems, November 15-16, 2001, Brussels, Belgium. Springer, 2002.
24. GERTZ, M., GULDENTOPS, E., STROUS, L., (ed.)., Integrity, internal control and security in information systems: connecting governance and technology, IFIP TC11/ WG11.5 Fourth Working Conference on Integrity and Internal Control in Information Systems, November 15-16, 2001, Brussels, Belgium. Springer, 2002., str. 3 -10.
25. GHONAIMY, M. A. R., EL-HADIDI, M.T., ASLAN, H.K., Security in the information society: visions and perspectives, IFIP TC11 17th International Conference on Information Security (SEC2002), May 7-9, 2002, Cairo, Egypt, Springer, 2002.
26. GOLDENBERG, B. J., CRM in Real Time: Empowering Customer Relationships, Information Today, Inc., 2008.
27. IACOVINI, J., The human side of organization change, Training & Development, 47(1), str. 65 – 68.
28. QUIGLEY, M., Encyclopedia of information ethics and security, Idea Group Inc (IGI), 2008.
29. KATULIĆ, T., Stiže Opća uredba o zaštiti podataka, dostupno na: http://www.bug.hr/molex/general-data-protection-regulation/97346.aspx.
30. KIZZA, J. M., A Guide to Computer Network Security, Springer, 2008.
31. KOVAČEK, M., Važne stvari koje morate znati o Zakonu o zaštiti osobnih podataka (General Data Privacy Regulation – GDPR), dostupno na: https://hitkonferencijablog.com/2017/06/20/vazne-stvari-koje-morate-znati-o-zakonu-o-zastiti-osobnih-podataka-general-data-privacy-regulation-gdpr/ .
32. MACHLUP, F., Knowledge: its Creation, Distribution and Economic Significance, vol. III, The Economics of Information and Human Capital, Princeton, NJ, Princeton University Press, 1984.
33. MILLER, F. P, VANDOME, A. M., MCBREWSTER, J., Digital Signature: Electronic Signature, Public- Key Cryptography, Signature, E- Mail, Contract, Cryptographic Protocol, Bit Array, Global Trust Center, Cryptography, Alphascript Publishing, 2010.
34. MULGAN, G., Communication and Control: Networks and the New Organizations, Helsinki: Metaxis, 1991.
35. NANAVATI, S., THIEME, M., NANAVATI, R., Biometrics: identity verification in a networked world, John Wiley & Sons, 2002.
36. Nova regulacija zaštite podataka, Comping d.o.o., slide 8., dostupno na: http://www.comping.hr/easyedit/UserFiles/GDPR/gdpr-brosura-screen.pdf .
37. Opća uredba o zaštiti osobnih podataka, Središnji državni ured za razvoj digitalnog društva, dostupno na: https://rdd.gov.hr/UserDocsImages//dokumenti//GDPR%20%20Op%C4%87a%20Uredba%20o%20za%C5%A1titi%20osobnih%20podataka.pdf.
38. PANIAN, Ž., Kontrola i revizija informacijskih sustava, Sinergija, Zagreb, 2001.
39. PANIAN, Ž., Izazovi elektroničkog poslovanja, Narodne novine, Zagreb, 2002.
40. PAVLOV, A., NATHAN VAN DE WOUW, N. VAN DE W., NIJMEIJER, H., Uniform

output regulation of nonlinear systems: a convergent dynamics approach, Springer, 2006.
41. PINTELON, R., SCHOUKENS, J., System identification: a frequency domain approach, John Wiley and Sons, 2001.
42. Povelja Europske unije o temeljnim pravima, 2007/C 303/01.
43. RADOLOVIĆ, A., Pravo osobnosti u novom Zakonu o obveznim odnosima, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Vol. 27, br. 1, 2006., str. 129-170.
44. RAGHENO, N. (dir.), Collectif, Data Protection & Privacy: Le GDPR dans la pratique - De GDPR in de praktijk, Anthemis, 2017.
45. 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).
46. RUSTICI, C., Applying the GDPR: The Functional Specifications of Eu-Grade Privacy, O'Reilly Media, 2017.
47. ŠIMOVIĆ, V., ŠIMUNDIĆ, S., BAČA, M., Policija i informatika, Ministarstvo unutarnjih poslova, Zagreb, 1998.
48. TUĐMAN, M., Teorija informacijske znanosti, Informator, Zagreb, 1990.
49. TUNG, B., Kerberos: a network authentication system, Addison-Wesley, 1999., str. 93. Vidi i GARMAN, J., Kerberos: the definitive guide, O'Reilly Media, Inc., 2003.
50. TUOMI, I., Corporate Knowledge: Theory and Practice of Intelligent, 1999.
51. Ustav Republike Hrvatske (Narodne novine, br. NN 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.
52. VOIGT, P., BUSSCHE VON DEM, A., The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017.
53. WRYCZA, S., Systems Analysis and Design for Advanced Modeling Methods: Best Practices, IGI Global snippet, 2009.
54. YORAV, K., (Ed.), Hardware and software, verification and testing, Third International Haifa Verification Conference, HVC 2007, Haifa, Israel, October 23-25, 2007, Proceedings, Springer, 2008.
55. Zakon o medijima (Narodne novine, br. 59/04, 84/11, 81/13).
56. Zakon o o zaštiti osobnih podataka (Narodne novine, br. 103/03, 118/06, 41/08, 130/11, 106/12).
57. Zakon o udrugama, (Narodne novine, br. 74/14, 70/17).

Jozo Čizmić*

Marija Boban**

Summary

IMPACT OF NEW EU GENERAL DATA PROTECTION REGULATION 2016/679 (GDPR) ON THE PROTECTION OF PERSONAL DATA IN THE REPUBLIC OF CROATIA

After more than seven years from the initial initiative and four years of negotiations, the new EU General Protection Regulation was finally adopted in April 2016. In full name 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 (here and after GDPR) replaces the current EU Directive 95/46/EZ and comes into force on the date of adoption and is directly applicable in all EU Member States. The ability to adapt certain parts is still left in national legislation as of May 25, 2018, when GDPR starts to apply!The key assumption of the development of the contemporary digital economy is based on the accelerated development of information and communication technologies, at the same time creating new challenges and threats to privacy and the protection of personal data. Data processing, especially personal data processing, new information and communication tools and the digital market, have developed the need to increase privacy protection of new digital products and services. The solution is mentioned in the new EU data protection framework called GDPR. The Regulation introduces major changes in personal data management and applies directly to all organizations that have personal data of EU citizens. Also, GDPR brings significant changes to the rules that define personal information and defines new concepts as well as compliance, planning, implementation and compliance compliance, as well as performance appraisal. In some cases the organization will also need to appoint a qualified Data Protection Officer who will be directly responsible to the Administration. Institutions and companies are required to complete alignment by May 25, 2018 - then the GDPR will come into force throughout the European Union. In this paper, authors will present the impact assessment of the new EU Data Protection Regulation and the legal remedies obligatory to the public and private sector in the implementation of GDPR, which will provide the modernized data protection framework in Europe. The new rules will establish the new European Data Protection framework introducing a new definition of personal data and replacing current inconsistent national laws with a view to increasing the level of data protection

* Jozo Čizmić, Ph. D., Full Professor, Faculty of Law, University of Split; Jozo.Cizmic@pravst.hr.

** Marija Boban, Assistant Professor, Faculty of Law, University of Split; marija.boban@gmail.com.

and increasing legal certainty in the growing digital economy.

Keywords: *GDPR, personal data, data processing, data protection, data protection officer, EU data protection, EU law, information and communication tehcnologies, impact assessment, legal remedies, pseudonymization, privacy.*

Zussamenfassung

AUSWIRKUNG DER NEUEN VERORDNUNG (EU) 2016/679 (GDPR) AUF DEN SCHUTZ PERSONENBEZOGENER DATEN IN DER REPUBLIK KROATIEN

Nach mehr als sieben Jahren seit der Initiative dazu und nach vier Jahren von Verhandlungen wurde im April 2016 endlich der neue europäische Datenschutzrahmen verabschiedet. Die allgemeine Verordnung (EU) 2016/679 zum Schutz personenbezogener Daten oder GDPR (General Data Protection Regulation) hebt die Richtlinie 95/46/EG auf und wird direkt in alllen EU-Mitgliedstaaten angewandt. EU-Mitgliedstaaten andererseits dürfen Änderungen mancher Vorschriften vorschlagen und sie bis zum 25. Mai 2018 (Inkrafttreten der GDPR) der Kommission mitteilen.

Die Entwicklung moderner digitaler Ökonomie beruht auf schneller Entwicklung der Informations- und Kommunikationstechnologie, aber gleichzeitig schafft sie neue Herausforderungen und Gefahren für den Schutz personenbezogener Daten. Die Datenverarbeitung, insbesondere die Verarbeitung personenbezogener Daten, neue IT-Tools und digitale Märkte haben das Bedürfnis nach Erhöhung des Schutzes personenbezogener Daten bei neuen digitalen Produkten und Diensten geweckt. Die Lösung dazu wurde in der neuen Reform des europäischen Datenschutzrahmens angeboten, welcher große Änderungen im Bereich der Verarbeitung personenbezogener Daten einführt und wird direkt an alle mit personenbezogenen Daten der EU-Bürger verfügenden Vereinigungen angewandt. Ebenfalls führt die GDPR wesentliche Änderungen in den Regeln zur Definierung personenbezogener Daten ein und definiert sowohl neue Begriffe als auch die schon bekannten Begriffe der Angleichung, Planung, Umsetzung, Aufrechterhaltung der Angleichung und Auswirkungsbewertung. In manchen Fällen sollten die Vereinigungen den Datenschutzbeauftragten (DPO – Data Protection Officer) ernennen, der direkt den höchsten Managementebene berichtet. Stiftungen und Unternehmen müssen die Angleichung bis zum 25. Mai 2018 beenden, wenn die GDPR in allen EU-Mitgliedstaaten in Kraft tritt.

Diese Arbeit stellt die Bestimmungen und die Anwendung der neuen Verordnung (EU) zum Schutz personenbezogener Daten sowie auch die Bestimmungen des öffentlichen und privaten Sektors zur GDPR-Umsetzung unter besonderer Berücksichtigung der Bewertung ihrer Auswirkung dar.

Neue Regeln werden zum europäischen Datenschutzrahmen beitragen, indem sie

die neue Definition personenbezogener Daten einführen und uneinheitliche nationale Gesetze ersetzen, alles mit dem Ziel den Datenschutz und die Rechtssicherheit in der Zeit der ständig fortschreitenden Entwicklung digitaler Ökonomie zu erhöhen.

Schlüsselwörter: *GDPR, personenbezogene Daten, Sanktionen, Pseudonymisierung, das Recht auf Vergessenwerden, Datenverarbeitung, Datenschutzbeauftragter, Angleichung, Auswirkung, Datenschutz.*

Riassunto

L'EFFICACIA DEL NUOVO REGOLAMENTO UE 2016/679 (GDPR) SULLA PROTEZIONE DEI DATI PERSONALI NELLA REPUBBLICA DI CROAZIA

Dopo più di sette anni dalla proposta iniziale e dopo quattro anni di trattative, finalmente nell'aprile del 2016 è stato emanato il nuovo quadro normativo in materia di protezione dei dati personali. Il Regolamento UE sulla protezione dei dati personali 2016/679 o anche noto come GDPR (*General Data Protection Regulation*) sostituisce l'attuale direttiva UE e si applica direttamente in tutti gli Stati Membri dell'UE. Tuttavia, viene lasciata ai singoli legislatori nazionali la possibilità di adeguamento di alcune parti fino al 25 maggio 2018, data in cui il GDPR entrerà in vigore!

Il presupposto fondamentale dello sviluppo dell'economia digitale contemporanea si basa sullo sviluppo delle tecnologie dell'informazione e della comunicazione; al tempo stesso, ciò crea nuove sfide e nuove insidie per la *privacy* e per la protezione dei dati personali. Il trattamento dei dati, in particolare dei dati personali, come i nuovi strumenti IT ed il mercato digitale, impongono la necessità di un innalzamento della protezione della *privacy* nell'ambito dei nuovi prodotti e dei servizi digitali. La soluzione è indicata nella nuova riforma UE nell'ambito della protezione dei dati personali, la quale introduce grandi cambiamenti nel modo di amministrare i dati personali, applicandosi direttamente a tutte le organizzazioni che dispongono di dati personali dei cittadini dell'Unione europea. Altresì, il GDPR porta con sé significativi cambiamenti nelle regole che determinano i dati personali e definisce le nuove nozioni, come pure l'adeguamento ed il suo mantenimento, la pianificazione, l'attuazione e la valutazione degli effetti. In alcuni casi le organizzazioni dovranno nominare un responsabile qualificato per la protezione dei dati personali (DPO – *Data Protection Officer*) il quale risponderà direttamente all'amministrazione. Gli enti e le società hanno l'obbligo di concludere l'adeguamento entro il 25 maggio 2018, quando il GDPR entra in vigore nell'intera Unione europea.

In questo lavoro gli autori presenteranno le disposizioni e l'applicazione del nuovo Regolamento UE sulla protezione dei dati personali ed illustreranno le disposizioni rilevanti tanto nel settore pubblico, che in quello privato in occasione

dell'applicazione del GDPR, prestando attenzione alla valutazione dell'efficacia che garantirà un quadro moderno per la protezione dei dati in Europa. Le nuove regole porranno il fondamento per la legislazione europea sulla protezione dei dati personali, sostituendo le attuali contradditorie legislazioni nazionali al fine di innalzare la soglia della protezione dei dati personali, come anche di aumentare la certezza del diritto nella crescente economia digitale.

Parole chiave: *GDPR, dati personali, sanzioni, pseudonimizzazione, diritto all'oblio, trattamento dei dati, responsabile per la protezione dei dati, adeguamento, efficacia, protezione dei dati.*