Andrej Diligenski
Dragan Prlja Dražen Cerović

PRAVO ZAŠTITE PODATAKA

GDPR

Institut za uporedno pravo Beograd
2018

Andrej Diligenski
Dragan Prlja
Dražen Cerović

PRAVO ZAŠTITE PODATAKA
GDPR

Institut za uporedno pravo
Beograd
2018

INSTITUT ZA UPOREDNO PRAVO

PRAVO ZAŠTITE PODATAKA GDPR

Izavač:
Institut za uporedno pravo
Beograd, Terazije 41

Za izdavača:
Vladimir Čolović

Recenzenti:
Prof. dr Stevan Lilić
Prof. dr Gordana Gasmi
Prof. dr Mario Reljanović
Prof. dr Miodrag Savović

Lektura i korektura
Sanja Prlja

ISBN:978-86-80186-42-9

Štampa:
Planeta Print, Beograd

*Tiraž:*500

INSTITUTE OF COMPARATIVE LAW

DATA PROTECTION LAW GDPR

Published by:
Institute of Comparative Law
Belgrade, Terazije Street 41

For the Publisher:
Vladimir Čolović

Reviewed by:
Prof. Stevan Lilić Ph. D.
Prof. Gordana Gasmi Ph. D.
Prof. Mario Reljanović Ph. D.
Prof. Miodrag Savović Ph. D.

Proofreading
Sanja Prlja

ISBN: 978-86-80186-42-9

Printing:
Planeta Print, Belgrade

*Copies:*500

SADRŽAJ

"Mi znamo, gde si ti. Mi znamo, gde si bio. Mi manje više znamo o čemu ti misliš."

Izvršni direktor Gugla Eric Schmidt

Intervju sa James Bennetom (The Atlantic) na "Second Annual Washington Ideas Forum-u" 1. oktobra 2010. godine

1. UVOD

Razvoj informacionih tehnologija danas, pored niza pozitivnih efekata prouzrokovao je i neverovatan rast zbirki podataka o gotovo svim pojedincima širom sveta. Milijarde podataka u svakom trenutku se prikupljaju u virtuelnom svetu, prodaju se kao roba, zloupotrebljavaju se na mnogobrojne načine. Svaki pojedinac suočen je sa činjenicom da razne državne institucije, privatne kompanije i pojedinci prikupljaju, obrađuju i koriste njegove lične podatke. Zbog neverovatne lakoće i brzine kojom se podaci mogu prikupiti i zloupotrebiti, i velikog broja pojedinaca koji time mogu biti pogođeni jedno od najvažnijih pitanja 21 veka je *pitanje zaštite podataka*. Njime se sa različitih aspekata moraju baviti stručnjaci i iz prirodnih i društvenih nauka. Upotreba veštačke inteligencije i sofisticiranih softverskih rešenja prilikom prikupljanja i obrade podataka samo uvećavaju broj novih pitanja koja se direktno reflektuju na svakog pojedinca. Psihološke i sociološke posledice ovakvog razvoja situacije po pitanju upotrebe i zloupotrebe ličnih podataka nisu još uvek u potpunosti sagledive. Kako ispravno zaključuje Džulijan Asanž najmoćnije sredstvo za kontrolu i nadgledanje pojedinaca danas je internet.[1] Kada privatna kompanija uz pomoć interneta poseduje milijarde podataka i informacija među kojima su i one o političkom ubeđenju, seksualnoj orjentaciji, kretanju u digitalnom svetu, imovinskom stanju, obrazovanju, zdravstvenim problemima, profesionalnom angažovanju pojedinaca, onda mnogi počinju da se pitaju kako da se pojedinac odbrani od nadzora i kontrole koja se vrši nad njegovom privatnošću.

Ovako značajne promene u društvenim odnosima uvek su pratile i promene u pravnim propisima. Sve sfere društvenih odnosa moraju biti adekvatno regulisane pravnim propisima. Promene u društvenim odnosima koje su danas uslovljene izuzetno brzim tehnološkim razvojem stavljaju pravo pred mnogobrojne izazove u različitim

[1] Ben Mezrih, *Slučajni milijarderi : nastajanje Fejsbuka*, Beograd: Evro-Giunti, 2010, str. 174.

oblastima. Sfera privatnosti i njeno klasično shvatanje krajem devetnaestog veka, kao pravo pojedinca da bude ostavljen na miru, odnosno da ima pravo da njegova intimna sfera ne bude dostupna javnosti odavno je prevaziđeno.[2] Danas je pravna regulativa sve više usmerena ka tome da zaštiti pojedinca od nepoželjne obrade podataka, odnosno da zaštiti interese pojedinaca koji su u vezi sa njegovim podacima.[3] Određivanje koncepta privatnosti danas više se vezuje za kontrolu informacija i praktično ostvarivanje tog prava.[4] Pojedinac može da se zaštiti od opasnosti koje nove tehnologije sa sobom donose, ako mu se pravno prizna i zaštiti mogućnost da zna za informacione tokove podataka o njemu, da ima mogućnost da ih nadzire, i da utiče na njih.[5] Pravo treba pojedincima da garantuje da znaju i kontrolišu ko koristi informacije o njima, kada i u koje svrhe, da li imaju ovlašćenja za to, da znaju li je došlo do promene tih informacija, zašto i u koje svrhe.[6] Pravna regulativa zaštite podataka danas ima dva glavna zadatka. Prvi je da uredi prava i obaveze onih koji prikupljaju i obrađuju podatke o ličnosti. Drugi je da ustanovi kakva prava u vezi sa ličnim podacima pojedinci imaju i kako ih mogu ostvariti.[7]

Možemo konstatovati da je danas zaštita podataka fundamentalno ljudsko pravo koje po svojoj širini daleko prevazilazi koncept prava na privatnost uobličen Univerzalnom deklaracijom o ljudskim pravima Ujedinjenih nacija 1948. godine i Evropskom konvencijom za zaštitu ljudskih prava i osnovnih sloboda Saveta Evrope 1950.g. Prema članu 12 Univerzalne deklaracije o ljudskim pravima "Niko se ne sme izložiti proizvoljnom mešanju u privatni život, porodicu, stan ili prepisku niti napadima na čast i ugled.". Prema članu 8. Evropske konvencije za zaštitu ljudskih prava i sloboda "Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske.".[8] Teorijska shvatanja prava privatnosti, njegovog značenja, kao i načina zaštite u velikoj meri se razlikuju u odnosu na anglosaksonski sistem prava i evropsko kontinentalni sistem prava. Privatnost se danas u evropsko kontinentalnom sistemu prava deli na tri sfere privatnosti. Prva je *tajna sfera* u koju spadaju skriveni intimni podaci koje pojedinac drži u strogoj tajnosti. Druga sfera je *privatna sfera* u koju spadaju podaci nešto poznatiji porodici, prijateljima, kao što su podaci o zdravstvenom stanju, poslovanju, verskom ili političkom opredeljenju, životnim planovima, hobijima, itd. U treću sferu spadaju *privatno-javni* podaci, to su podaci koji se se mogu saznati na javnom mestu, kao što je ulica, bioskop, hotel. itd.[9] Podelu

---

[2] Paul Lambert, *Understanding the New European Data Protection Rules*, CRC Press, Boca Raton, 2018, str. 9.

[3] Vladimir Vodinelić, *Obrada podataka i zaštita ličnosti*, Anali Pravnog fakulteta, br. 2-3/1989, str. 189.

[4] Stevan Lilić, *Pravo, informatička tehnologija i zaštita podataka*, Anali Pravnog fakulteta, br. 2-3/1989, str. 217.

[5] Vladimir Vodinelić, *Pravo zaštite ličnih podataka*, u Nebojša Šarkić, i dr. "Pravo informacionih tehnologija", Pravni fakultet Univerziteta Union, 2007, str. 150.

[6] Predrag. Dimitrijević, *Pravo informacione tehnologije*, SVEN, Niš 2010, str. 250.

[7] David Bainbridge, *Introduction to Computer Law*, Longman, London 2000, str. 361.

[8] Miodrag Savović, *Internet i zaštita prava na privatnost*, u Dragan Todorović, Dalibor Petrović, Dragan Prlja, "Internet i društvo", Srpsko sociološko društvo, Univerzitet u Nišu Filozofski fakultet, Institut za uporedno pravo, Niš, 2014, str. 366.

[9] Dragica Popesku, *Zaštita prva privatnosti i njegove sfere*, Strani pravni život, br. 1/2016, str. 78.

na javnu i privatnu sferu definisao je još Aristotel u svom delu "Politika" smatrajući da se privatna sfera vezuje za lični i porodični život pa ce tiče samo pojedinca, ili grupe pojedinaca, a ne društva u celini.[10] Ove teorijske podele svakako doprinose razjašnjenju pojma privatnosti, ali prilikom ostvarivanja zaštite kada je privatnost ugrožena, mora se pojedinačno odmeravati interes svake osobe za očuvanje njene privatnosti, istovremeno odmeravajući interes drugih da u tu privatnost uđu, na primer radi ostvarivanja javnog interesa.[11]

Uporedo sa razvojem teorija o shvatanju privatnosti i zaštitom prava privatnosti pred sudovima u Evropi se od sedamdesetih godina dvadesetog veka pa sve do danas razvijala pravna regulativa koja uređuje pitanje zaštite podataka i stvara kompleksan sistem zaštite podataka. U početku su to bili zakonski propisi pojedinih evropskih zemalja, a potom je glavnu ulogu u stvaranju sistema zaštite podataka preuzela Evropska Unija. Od velikog broja propisa koji su doneti u okviru Evropske unije treba izdvojiti pre svega Direktivu o zaštiti podataka (Directive 95/46/EC),[12] Direktivu o privatnosti i elektronskim komunikacijama (Directive 2002/58/EC),[13] Direktivu kojom se menja Direktiva o privatnosti i elektronskim komunikacijama (Directive 2006/24/EC),[14] Direktivu kojom se takođe menja Direktiva o privatnosti i elektronskim komunikacijama (Directive 2009/136/EC),[15] i Telekom paket Direktivu (Directive 2009/140/EC).[16]

Stupanjem na snagu Lisabonskog sporazuma 1. decembra 2009. godine pravnu obaveznost i isti pravni značaj kao i osnivački ugovori stekla je Povelja Evropske unije o osnovnim pravima usvojena 2000. godine i izmenjena 2007. godine koja članom 8. definiše pravo na zaštitu podataka:

[10] Dušan Popović, Marko Jovanović, *Pravo interneta: odabrane teme*, Univerzitet u Beogradu - Pravni fakultet, Beograd, 2017, str. 123.

[11] *Ibidem*, str. 79.

[12] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, *Official Journal L 281 , 23/11/1995.*

[13] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, *Official Journal L 201 , 31/07/2002.*

[14] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105 , 13/04/2006.*

[15] *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws,* Official Journal L 337 , 18/12/2009.

[16] *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, Official Journal L 337 , 18/12/2009.*

" (1) Svako ima pravo na zaštitu ličnih podataka koji ga se tiču.

(2) Takvi podaci moraju da se obrađuju na pravičan način, u tačno određene svrhe i na osnovu saglasnosti lica kojeg se tiče, odnosno lica koje za to ima legitiman, zakonom priznat interes. Svako ima pravo da pristupi prikupljenim podacima koji ga se tiču i da traži ispravku takvih podataka.

(3) O poštovanju ovih pravila staraće se nezavisno telo".[17]

U okviru razvoja prava na zaštitu podataka u Evropskoj uniji poseban značaj je imala direktiva koja se u potpunosti odnosi na zaštitu podataka, doneta je još 1995. godine. Ova direktiva je bila kamen temeljac u razvitku daljih pravnih propisa EU u oblasti zaštite podataka i prava privatnosti, pre svega zato što je dugogodišnja sudska praksa bazirana na ovoj direktivi.[18] Ostale direktive predstavljaju nadogradnju kako bi se omogućila primena ovih direktiva u oblasti elektronskih komunikacija. Direktiva iz 1995. godine poslužila je kao baza za donošenje 2016. g. Opšte uredbu o zaštiti podataka (Regulation 2016/679), koja je počela da se primenjuje 25.5.2018. godine.[19]

Naša knjiga ima za cilj da čitaoce upozna sa Opštom uredbom o zaštiti podataka (u daljem tekstu "OUZP"), poznatijom kao GDPR. Osim toga cilj ove knjige je da pomogne kako privatnom tako i javnom sektoru u usklađivanju sa OUZP, pošto sadrži sve obaveze za rukovaoce i obrađivače, koji su predviđeni u OUZP. Inače se radi o vrlo složenom i za našu pravnu struku prilično nerazumljivom tekstu pravnog propisa koji ima već sada globalne efekte i mogućnost primene u svim zemljama širom sveta.[20] Zbog ovog pravnog propisa milioni kompanija menjaju svoje ponašanje i način funkcionisanja među kojima i one najveće, poput Gugla ili Fejsbuka. Takođe veliki broj država širom sveta menja svoja nacionalna zakonodavstva i usklađuje ih sa OUZP, a građani dobijaju bolju zaštitu i nova prava, koja sada mogu i da ostvare.

Autori

---

[17] Dušan Popović, Marko Jovanović, *Pravo interneta: odabrane teme*, Univerzitet u Beogradu - Pravni fakultet, Beograd, 2017, str. 130.

[18] Nataša Tomić, Dalibor Petrović, *Društveno umrežavanje i zaštita privatnosti korisnika interneta*, Saobraćajni fakultet Univerziteta u Beogradu, XXVII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2009, Beograd, 15. i 16. decembar 2009. http:// postel. sf. bg. ac. rs/ downloads/ simpozijumi/ POSTEL2009/ RADOVI%20PDF/ Menadzment%20procesa% 20u%20 postanskom% 20i%20telekomunikacionom%20saobracaju/9.%20N.%20Tomic,%20D.%20Petrovic. pdf, 07.08.2012, str. 97.

[19] *Regulation 2016/679 of the European Parliament and of the Council of 7 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, p. 1–88.*

[20] Tako je primera radi Kina u sopstveni pravni sistem integrisala suštinske elemente i principe OUZP. Prof. Dr. Jürgen Kühling, RA Florian Sackmann, *Rechte an Daten*, Verbraucherzentrale Bundesverband e.V., novembar 2018., str. 5.

2. OPŠTA UREDBA O ZAŠTITI PODATAKA (OUZP)

2.1. Uvod

Pravni sistem zaštite podataka u Evropi zasnovan na Direktivi o zaštiti podataka iz 1995. godine nije bio dovoljan da bi na adekvatan način odgovori na ubrzani razvoj tehnologije i mnogobrojne načine neadekvatnog prikupljanja i obrade podataka o ličnosti pa je iz tog razloga januara 2012. godine započeta zakonodavna procedura za donošenje uredbe koja bi na sveobuhvatan način regulisala pitanja prava na zaštitu podataka. Nakon duge javne diskusije i usaglašavanja mnogobrojnih predloga i razmatranja preko 4.000 amandmana aprila 2016. godine usaglašen je i usvojen tekst Opšte uredbe o zaštiti podataka.[21] Zbog kompleksnosti propisa i neophodnosti prilagođavanja institucija koje moraju da ga primene ostavljen je period od 2 godine do početka primene, pa je ovaj propis počeo da se primenjuje od 25. maja 2018. godine.

OUZP znatno je obimnija od Direktive iz 1995. godine i ima 173 uvodne tačke razmatranja (u daljem tekstu "U.t.r.") i 99 članova, a takođe donosi i novi stepen obaveznosti, jer se direktno primenjuje u svim državama članicama EU. Ovoliki broj uvodnih tački razmatranja je prisutan iz razloga što se države članice EU nisu mogle usaglasiti oko mnogih pitanja. Na taj način su one izbačene iz obavezujućeg dela OUZP, ali njihovo dejstvo ne treba zanemariti, pošto će se sudovi često u svojim odlukama i tumačenjima pozivati na njih.[22] Stoga će one i u knjizi poslužiti za tumačenje pojedinih članova OUZP.

Osnovni cilj OUZP je da se obezbedi poštovanje svih osnovnih prava i sloboda, a posebno poštovanje privatnog i porodičnog života, komunikacije, zaštite ličnih podataka, sloboda mišljenja, veroispovesti, sloboda izražavanja i informisanja, sloboda preduzetništva, pravo na efikasan pravni lek i pošteno suđenje, kao i pravo na kulturnu, versku i jezičku različitost. OUZP je ima za cilj da obezbedi i pravnu sigurnost i transparentnost, kao i jednaki nivo prava, obaveza i odgovornosti pojedinaca i institucija koje vrše obradu ličnih podataka, kao i jednake sankcije u svim državama članicama EU.

OUZP se ne odnosi na obradu ličnih podataka povezanu sa nacionalnom bezbednošću, pitanjima zajedničke spoljne i bezbedonosne politike EU i sa obradom ličnih podataka u svrhu sprečavanja i otkrivanja krivičnih dela, ali se odnosi na obradu ličnih podataka koje obavljaju institucije i organi EU.[23]

Neki od ciljeva donošenja OUZP bili su takođe usklađivanje sa tehnološkim razvojem i potreba unifikacije različitih propisa iz oblasti zaštite podataka država

---

[21] Dušan Pavlović, *Uredba Evropske unije o zaštiti podataka o ličnosti,* http://pravoikt.org/uredba-evropske-unije-o-zastiti-podataka-o-licnosti/, 06.12.2018.

[22] Maximilian Schrems, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 34.

[23] Sanja Prlja, *Pravo na zaštitu ličnih podataka u EU*, Strani pravni život, Institut za uporedno pravo, Beograd, br. 1/2018, str. 92.

članica EU na nacionalnom nivou.[24] Razvojem tehnologije obim prikupljanja i razmene podataka o ličnosti značajno se povećao. Tehnologija je omogućila privatnim kompanijama i institucijama vlasti da koriste podatke o ličnosti u do sada nezabeleženom obimu, a pojedinci svoje lične podatke sami čine javno dostpnim pa je to svakako bio jedan od razloga potrebe obezbeđivanje što višeg nivoa zaštite podataka.

OUZP u cilju stvaranja efikasnog sistema zaštite podataka definiše ko su učesnici u tom procesu: *pojedinci* čiji se podaci prikupljaju i obrađuju, *institucije rukovaoci* koje prikupljaju i obrađuju lične podatke, *spoljne institucije obrađivači* kojiima su rukovaoci delegirali neke aktivnosti prikupljanja ili obrade podataka, *ovlašćeno lice za zaštitu podataka* koje je u organizaciji zaduženo da obezbedi usklađenost sa zahtevima OUZP, *nadzorni organ* za zaštitu podataka na nacionalnom nivou, *Evropski odbor za zaštitu podataka* kao organ na nivou EU zadužen za usklađivanje i tumačenje prava zaštite podataka.[25]

Neka od novih prava i obaveza koji su definisani OUZP su: novi ili izmenjeni osnovni principi kao što su pravičnost i zakonitost, transparetnost, tačnost, itd., nove definicije ključnih pojmova, ovlašćena lica za zaštitu podataka, posebna pravila koja se odnose na maloletna lica, nov način primene i nove sankcije, pravo na digitalni zaborav, pravo na prenosivost podataka, propisi vezani za bezbednost i "curenje" podataka, procena rizika, itd.[26]

Jedan od značajnih ciljeva OUZP je podizanje nivoa bezbednosti podataka pa se tako predviđaju tehničke i organizacione mere neophodne da bi se mogla obezbediti usaglašenost sa OUZP, među kojima se posebno izdvaja kao cilj podsticanje primene pseudnimizacije prilikom obrade podataka oličnosti.

Direktna primena OUZP ipak ne isključuje donošenje nacionalnih propisa iz oblasti zaštite podataka. Nacionalni zakoni u ovoj oblasti su neophodni jer OUZP ostvalja veliki broj *otvorenih klauzula* kojima se preciziraju mnoga bitna pitanja, o čemu će detaljnije biti reči u poglavlju 2.4. ove knjige.[27]

OUZP je podeljena na jedanaest poglavlja.

Prvo poglavlje OUZP pod nazivom *"Opšta načela"* sadrži četiri člana koji definišu pitanja predmeta i cilja, područja primene, teritorijalnog važenja, i dvadesetšest definicija.

Drugo poglavlje OUZP pod nazivom *"Načela"*, sadrži sedam članova koji regulišu pitanja načela obrade podataka o ličnosti, zakonitost obrade, uslove za pristanak, uslove koji se primenjuju na pristanak deteta u vezi sa uslugama informacionog društva, obrade posebnih kategorija podataka o ličnosti, obrade

[24] Dejan Đukić, *Zaštita podataka o ličnosti sa osvrtom na novo zakonodavstvo EU u ovoj oblasti*, Pravni zapisi, Pravni fakultet Univerziteta Union, Beograd, br. 1/2017, str. 58.

[25] Paul Lambert, *Understanding the New European Data Protection Rules*, CRC Press, Boca Raton, 2018, str. 62-63.

[26] *Ibidem*, str. 102.

[27] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017., str. 220-222.

podataka o ličnosti koji se odnose na krivičnu i prekršajnu osuđivanost i obradu podataka za koju nije potrebna identifikacija.

Treće poglavlje OUZP pod nazivom *"Prava lica na koje se podaci odnose"* sadrži pet odeljaka sa ukupno dvanaest članova. Ti odeljci su: transparetnost i modaliteti, informacije i pristup podacima o ličnosti, ispravka i brisanje, pravo na prigovor i donošenje automatizovanih pojedinačnih odluka, i ograničenja.

Četvrto poglavlje OUZP pod nazivom *"Rukovalac i obrađivač podataka"* sadrži pet odeljaka sa dvadeset članova. Ti odeljci su: opšte obaveze, bezbednost podataka o ličnosti, procena uticaja u vezi sa zaštitom podataka i predhodne konsultacije, ovlašćeno lice za zaštitu podataka, i kodeks ponašanja i sertifikacija.

Peto poglavlje OUZP pod nazivom *"Prenosi podataka o ličnosti trećim zemljama ili međunarodnim organizacijama"* sadrži sedam članova koji regulišu pitanja: opšta načela prenosa, prenosa na osnovu odluke o adekvatnosti, prenos na koji se primenjuju odgovarajuće zaštitne mere, obavezujuća korporativna pravila, prenos ili otkrivanje podataka koji nisu dozvoljeni u pravu Unije, odstupanja u posebnim slučajevima, i međunarodne saradnje radi zaštite podataka o ličnosti.

Šesto poglavlje OUZP pod nazivom *"Nezavisni nadzorni organi"* sadrži dva odeljka sa osam članova. Ti odeljci su: nadzorni organ i nadležnost, zadaci i ovlašćenja.

Sedmo poglavlje OUZP pod nazivom *"Saradnja i konzistentnost"* sadrži tri odeljka i sedamnaest članova. Ti odeljci su: saradnja, konzistentnost, i Evropski odbor za zaštitu podataka.

Osmo poglavlje OUZP pod nazivom *"Pravna sredstva, odgovornost i sankcije"* sadrži osam članova koji regulišu pitanja: prava na pritužbu nadzornom organu, prava na delotvorno pravno sredstvo protiv nadzornog organa, pravo na delotvorno pravno sredstvo protiv rukovaoca ili obrađivača, zastupanja lica na koje se podaci odnose, privremeno obustavljanje postupka, pravo na naknadu štete i odgovornost, opšti uslovi za izricanje administrativnih novčanih kazni i sankcija.

Deveto poglavlje OUZP pod nazivoma *"Odredbe u vezi sa posebnim situacijama obrade"* sadrži sedam članova koji se odnose na pitanja: obrade i sloboda izražavanja i informisanja, obrade i pristup javnosti službenim dokumentima, obrade nacionalnog identifikacionog broja, obrade u kontekstu zaposlenja, zaštitne mere i odstupanja u vezi sa obradom u svrhe arhiviranja u javnom interesu u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, obaveze čuvanja tajnosti, i postojećih pravila o zaštiti podataka crkava i verskih udruženja.

Deseto poglavlje OUZP pod nazivom *"Delegirani akti i akti za sprovođenje"* sadrži dva člana koji regulišu pitanja delegiranja ovlašćenja i postupka odbora.

Jedanaesto poglavlje OUZP pod nazivom *"Završne odredbe"* sadrži šest članova koji regulišu pitanja stavljanja van snage Direktive 95/46/EZ, odnosa sa Direktivom 2002/58/EZ, odnosa sa predhodnim zaključenim sporazumima, izveštaja Komisije, preispitivanja drugih akata Unije o zaštiti podataka, i stupanja na snagu i primenu.

2.2. Materijalno područje primene (čl. 2 OUZP)

Da bi uopšte došlo do primene OUZP potrebno je ustanoviti i odgovoriti na pitanje stvarnog odnosno materijlnog područja primene OUZP.

„Ova se Uredba primjenjuje na *obradu podataka o ličnosti* koja se u celosti ili delimično obavlja *automatski ili neautomatski*, koja je snimljena u *zbirci podataka* ili je namenjena snimanju u zbirci podataka“ (čl. 2 st. 1 OUZP).

Materijalno područje primene obuhvata nekoliko važnih elemenata:

- ✓ Obradu (automatsku ili neautomatsku obradu podataka)
- ✓ Podatke o ličnosti
- ✓ Zbrika podataka

Prva 2 elementa odgovaraju na pitanje da li uopšte postoji primena OUZP. Da bi došlo da primene *neophodna je obrada* i *podaci o ličnosti*.

Definicija (čl. 4 br. 2 OUZP)

„*Obrada*” predstavlja svaki postupak ili skup postupaka, nezavisno od toga da li se radi o automatizovanim ili neautomatizovanim postupcima, koji se obavljaju u vezi sa podacima o ličnosti u šta spadaju prikupljanje, beleženje, organizacija, strukturisanje, snimanje, prilagođavanje ili izmena, pronalaženje, obavljanje uvida, upotreba, otkrivanje prenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili povezivanje, ograničavanje, brisanje ili uništavanje.

Potrebno je uočiti u ovoj definiciji pre svega širok spektar mogućnosti obrade, koja može biti automatska ili neautomatska. *Automatska obrada* se odnosi na pre svega korišćenje podataka u računarskim sistemima, mobilnim uređajima, tabletima itd., dok se *neautomatska obrada* odnosi na *manuelnu obradu podataka u papirnoj formi.*

Definicija „*podataka o ličnosti*“ je data u poglavlju 3.1. Može se reći da ukoliko ne postoji jedan od ova dva elemenata ne dolazi do primene OUZP, što naravno ne isključuje zavisno od zakonodavstva primenu drugih zakona iz oblasti privanosti, zaštite autorski prava, ličnih prava itd. Moraju dakle kumulativno biti ispunjena dva uslova: postojati obrada i postojati podaci o ličnosti. Stoga bi kontrolno pitanje trebalo da glasi:

Da li postoji materijalna primena OUZP?		
Dolazi do primene OUZP	Postoji obrada (čl. 4 br. 2 OUZP)	Radi se o podacima o ličnosti (čl. 4 br. 1 OUZP)
Ne dolazi do primene OUZP	Nema obrade podataka	Ne radi se o podacima o ličnosti

PRIMER POSTAVLJANJE VIDEO NADZORA BEZ FUNKCIJE
Samo postavljanje video nadzora bez funkcije (odnosno upotrebe) sa stanovišta OUZP ne predstavlja obradu, a takođe nema ni podataka o ličnosti. U sudskoj praksi odlučeno je od strane Vrhovnog suda Austrije da samo postavljanje video nadzora predstavlja zadiranje u lična prava pojedinca kao apsolutnog prava. I onda, kada kamera nije u funkciji, postoji prema mišljenju suda konkretan i opravdan strah, da bi kamera mogla u svakom trenutku biti uključena, navodi se u sudskoj odluci.[28]

Ovaj slučaj kao i procena prva dva elementa iz čl. 2 st. 1 OUZP nam je pokazao najčešću materijalnu stranu važenja OUZP. Postoji još jedan slučaj kada je neophodno da bude ispunjena definicija zbirke podataka (gore navedeni 3. element).

Definicija (čl. 4 br. 6 OUZP)

„*Zbirka podataka*" predstavlja svaku strukturisanu zbirku podataka o ličnosti dostupnih prema posebnim kriterijima, bilo da su centralizovani, decentralizovani ili raspršeni na funkcionalnoj ili geografskoj osnovi.

U navedenoj definiciji postoji naglasak na *strukturisanoj zbirci podataka*, koja je dostupna prema posebnim kriterijumima. Radi se takođe o tome da i ova zbirka podataka može biti obrađivana automastki ili neautomatski (manuelno).

PRIMER VIZIT KARTE
Na vizit karti su obično upisani ime, prezime, funkcija naziv fime, kontakt podaci. Iako se radi nesumljivo o podacima o ličnosti, ukoliko se vizit karte ne sortiraju po određenim kriterijumima, neće podpadati pod materijalnu primenu OUZP. To se naravno ne odnosi na dalju obradu ovih podataka u smislu ako se oni unesu sa vizit karte u kompjuter od strane fizičih lica. U tom slučaju može doći do primene OUZP, ako se ne radi o nekom od izuzetaka iz čl. 2 st. 2 OUZP (npr. u vidu korišćenja podataka isključivo u privatne ili familijarne svrhe).

Izuzetci od materijalne primene (čl. 2 st. 2, 3 i 4 OUZP):

- ✓ Delatnosti koje nisu obuhvaćene pravom EU (npr. nacionalna bezbednost);
- ✓ Delatnosti koje obavljaju države članice kada obavljaju aktivnosti koje su obuhvaćene područjem primene glave V. poglavlja 2. Ugovora EU (npr. aktivnosti vezane za spoljnu i bezbedonosnu politiku država članica EU);
- ✓ Aktivnosti koje vrši fizičko lice tokom isključivo privatnih ili familijarnih aktivnosti (npr. korišćenje društvenih mreža bez ekonomskih ciljeva, fotografisanje na rođendanskim proslavama bez ekonomskih ciljeva);[29]
- ✓ Delatnosti koju obavljaju nadležna tela u svrhu sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija,

[28] Andrej Diligenski, *Samo postavljanje video nadzora predstavlja zadiranje u lična prava pojedinaca,* Partneri za demokratske promene, http://partners-serbia.org/privatnost/ blog/samo-postavljanje-video-nadzora-predstavlja-zadiranje-u-licna-prava-pojedinaca/, 01.05.2018.

[29] Jörg Hladjk, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 40.

uključujući zaštitu i spečavanje opasnosti po javnu bezbednost;
- ✓ Obrada podataka o ličnosti koju obavljaju institucije, tela, organizacije i agencije Evropske Unije primenjuje se Uredba (EZ) br. 45/2001;
- ✓ Primena E-Commerce-Direktive 2000/31/EZ.

2.3. Teritorijalno područje primene (čl. 3 OUZP)

U pogledu teritorijalnog važenja OUZP treba razlikovati dve situacije:

- ✓ Kada se poslovno predstavništvo nalazi u EU
- ✓ Kada se poslovno predstavništvo nalazi izvan EU

U prvom slučaju se OUZP teritorijalno primenjuje na obradu podataka o ličnosti u okviru aktivnosti poslovnog predstavništva rukovaoca ili obrađivača u EU, nezavisno od toga da li se obrada obavlja u EU ili ne (čl. 3 st. 1 OUZP).

Obaveza primene OUZP pogađa dakle ili rukovaoca ili obrađivača koji ima poslovno predstavništvo u EU. Pritom nije od značaja da li se podaci obrađju u EU, sama činjenica da postoji *predstavništvo je odlučujuća tačaka vezivanja za primenu OUZP*.

Predstavništvo se odnosi na efektivno i stvarno obavljanje delatnosti putem stabilnih formi osnivanja. Pritom pravni oblik takvih formi osnivanja nije od značaja, bilo da se radi o podružnici odnosno ogranku ili društvu ćerki sa posebnom pravnom sposobnošću (U.t.r. 22 OUZP).

Može se reći da bilo koje preduzeće osnovano na teritoriji EU podleže OUZP nevezano za to da li je njegovo poslovanje uopšte usmereno na EU.

PRIMER FEJSBUK
Fejsbuk ima svoje predstavništvo u Irskoj. Time što se predstavništvo Fejsbuka nalazi na teritoriji EU dolazi do primene OUZP. Da li Fejsbuk vrši obradu podataka u Irskoj ili u SAD nije od značaja, da bi došlo do primene OUZP.

U drugom slučaju se OUZP teritorijalno primenjuje i onda kada se *poslovno predstavništvo nalazi izvan EU* pri obradi podataka o ličnosti koju obavlja rukovalac ili obrađivač, ako su aktivnosti obrade povezane sa:

- ✓ nuđenjem robe ili usluga pojedincima u EU, nezavisno od toga treba li pojedinac da izvrši plaćanje ili
- ✓ praćenjem ponašanja pojedinaca, dokle god se njihovo ponašanje odvija unutar EU.

Da bi se ustanovilo da li rukovalac ili obrađivač žele da ponude pojedincima na teritoriji EU *određenu robu ili usluge* potrebno je odgovoriti na pitanje: Da li postoji očigledna namera da se roba ili usluge ponude u EU?

U cilju odgovora na ovo pitanje a pre svega da bi se dokazala namera i došlo do primene OUZP, može poslužiti sudska praksa evropskog suda u oblasti međunarodnog javnog prava. Ukoliko se radi npr. o ponudi putem veb sajta se kao potencijalne tačke vezivanja mogu poslužiti određenja kao što su: *jezik* na kome se nudi roba ili usluge, *valuta* za plaćanje, korišćenje *internet domena* iz EU odnosno sa eu završetkom (npr. www.doktor.eu, www.doktor.it, www. doktor.at itd.), navođenje orijentacije aktivnosti sajta kao određenim klijentima u EU. Sama dostupnost veb sajta nije dovoljna tačka vezivanja da bi došlo do primene OUZP.[30]

Da bi se ustanovilo da li rukovalac ili obrađivač žele da *prate ponašanja pojedinaca u EU*, potrebno je ustanoviti sredstva i način takvih aktivnosti. Kao sredstva se nameću pre svega alati *BIG DATA*, dok se kao način mogu izrađivati *profili*. Tom prilikom se mogu iz raznih izvora analizirati podaci pojedinaca u EU i izrađivati profili na osnovu *radnog učinka, ekonomskog stanja, zdravlja, ličnih sklonosti, interesa, pouzdanosti, ponašanja, lokacijije ili kretanja*.

2.4. Pregled „otvorenih klauzula" shodno OUZP

OUZP ne reguliše sve situacije obrade podataka, stoga ovu uredbu mnogi nazivaju *tromom*. Sa druge strane intencija zakonodavca i nije bila da se regulišu sve situacije vezane za zaštitu podataka, već da se postavi pravni okvir. Tako OUZP i ostavlja brojne mogućnosti državama članicama da na nacionalnom nivou regulišu pojedina pitanja vezana za zaštitu podataka.[31]

Može se uočiti da OUZP sadrži norme koje države članice EU moraju uvesti u svoja zakonodavstva, dok takođe postoje norme koje države članice EU mogu da implementaraju u svojim zakonodavstvima.[32]

Član OUZP	*Područje regulisanja*	*Može/mora biti implementi-rano*
Čl. 4 br. 7	Dodeljivanje uloge rukovaoca, ukoliko su svrhe i sredstva obrade utvrđeni pravom EU ili pravom države članice	Može

[30] EuGH Urteil vom 7.12.2010, C-585/08, 144/09 – Peter Pammer ./. Reederei, Karl Schlüter GmbH & Co. KG und Hotel Alpenhof GesmbH ./. Oliver Heller, Euro Lawyer, strana 5, brojevi 93, 94, 95., http://www.eurolawyer.at/pdf/EuGH-C-585-08.pdf, 05.05.2018.

[31] Konrad Lachmayer, *Die DSGVO im öffentlichen Bereich*, Österreichische Juristen Zeitung, februar 2018, str. 118.

[32] Dr. Lukas Feiler, *Die 69 Öffnungsklauseln der DS-GVO*, Baker & McKenzie, http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf, 13.12.2018.

Čl. 4 br. 9	Tela javne vlasti koja mogu da prime podatke o ličnosti u okviru određene istrage u skladu sa pravom EU ili države članice ne smatraju se primaocima	Može
Čl. 6 st. 1 c) u vezi sa st. 2 i 3	Zakonitost obrade podataka, kada je obrada neophodna radi ispunjenja pravnih obaveza rukovaoca	Može
Čl. 6 st. 1 e) u vezi sa st. 2 i 3	Zakonitost obrade podataka, kada je obrada neophodna za izvršavanje zadataka od javnog interesa ili pri ispunjavanju javne vlasti rukovaoca	Može
Čl. 6 st. 4	Izuzetak od načela vezanosti za svrhu obrade podataka	Može
Čl. 8 st. 1	Niža starosna granica za pristanak deteta, koja može biti ispod 16 godina, ali ne niža od 13 godina	Može
Čl. 9 st. 2 a)	Ograničenje u davanju pristanka za obradu posebnih kategorija podataka	Može
Čl.9 st. 2 b)	Ograničenje obrade posebnih kategorija podataka u području radnog prava i prava socijalnog osiguranja	Može
Čl. 9 st. 2 g)	Ograničenje obrade posebnih kategorija podataka po osnovu nacionalnih zakonodavstava zbog značajnog javnog interesa	Može
Čl. 9 st. 2 h) u vezi sa st. 3	Ograničenje obrade posebnih kategorija podataka po osnovu nacionalnih zakonodavstava iz razloga preventivne medicine ili medicine rada, medicinske dijagnostike, pružanja zdravstvene ili socijalne zaštite, nege ili tretmana	Može
Čl. 9 st. 2 i)	Ograničenje obrade posebnih kategorija podataka po osnovu nacionalnih zakonodavstava iz razloga javnog zdravlja	Može
Čl. 9 st. 2 j)	Ograničenje obrade posebnih kategorija podataka po osnovu nacionalnih zakonodavstava u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe	Može
Čl. 9 st. 4	Uslovi i ograničenja u odnosu na obradu genetskih podataka, biometrijskih podataka ili zdravstvenih podataka	Može
Čl. 10	Izuzeci od opšte zabrane obrade podataka o kažnjavanju	Može
Čl. 14 st. 5 c)	Izuzetak od obaveze informisanja, ako je to izričito predviđeno nacionalnim pravom	Može
Čl. 14 st. 5 d)	Izuzetak od obaveze informisanja kod obveze čuvanja profesionalne tajne, ako je to predviđeno nacionalnim pravom	Može
Čl. 17 st. 1 e)	Obaveza brisanja podataka po osnovu zakonske obaveze	Može

Čl. 17 st. 3 b)	Izuzeci od obaveza brisanja podataka po osnovu zakonske obaveze ili zbog ispunjavanja zadataka od javnog interesa ili izvršavanja javne vlasti	Može
Čl. 22 st. 2 b)	Dopuštenost automatskih donošenja odluka i profilisanja	Može
Čl. 23	Ograničenja prava pojedinaca u svrhe javne bezbednosti, drugih važnih ciljeva od opšteg javnog interesa, zaštite pojedinaca ili prava i sloboda ostalih osoba, ostvarivanja potraživanja u građanskim sporovima	Može
Čl. 26 st. 1	Utvrđivanje obaveza zajedničkih rukovalaca shodno nacionalnim propisima	Može
Čl. 28 st. 3	Obrada podataka shodno nalogu koju sprovodi obrađivač uređuje se ugovorom ili drugim pravnim aktom u skladu sa pravom EU ili pravom države članice	Može
Čl. 28 st. 3 a)	Izuzetak od davanja naloga odnosno uputstava obrađivaču i u odnosu na prenos podataka u treće zemlje/međunarodne organizacije, ako je predviđen pravom EU ili države članice	Može
Čl. 28 st. 3 a)	Zabrana informisanja o obradi podataka rukovaoca od strane obrađivača iz razloga javnog interesa	Može
Čl. 28 st. 3 g)	Obaveza daljeg čuvanja podataka za obrađivača	Može
Čl. 28 st. 4	Kod angažovanja više obrađivača predviđaju se iste obaveze putem ugovora ili drugog pravnog akta ili shodno pravu države članice	Može
Čl. 29 i čl. 32 st. 4	Izuzetak u obradi podataka od strane obrađivača bez naloga ili uputa rukovalaca	Može
Čl. 35 st. 10	Izuzetak od obaveze sprovođenja procene uticaja u vezi sa zaštitom podataka kod zakonite obrade podataka	Može
Čl. 36 st. 5	Posebna obaveza konsultacije institucije za zaštitu podataka kao i dobijanje predhodnog odobređenja za obrade prilikom izvršenja zadataka u javnom interesu, obrade u vezi sa socijalnom zaštitom i javnim zdravljem	Može
Čl. 37 st. 4	Posebna obaveza angažovanja ovlašćenog lica za zaštitu podataka	Može
Čl. 40 st. 1	Države članice podstiču izradu kodeksa ponašanja posebno za mala i srednja preduzeća	*Mora*
Čl. 43 st. 1	Imenovanje sertifikacionog tela	*Mora*
Čl. 49 st. 1 d) u vezi sa st. 4	Prenos podataka u treću zemlju iz razloga javnog interesa	Može
Čl. 49 st. 1 g)	Prenos podataka u treću zemlju u cilju uvida javnosti vezanih za javne registre	Može

Čl. 49 st. 5	Ograničenje prenosa određenih kategorija podataka određenoj trećoj zemlji ili međunarodnoj organizaciji, ako ne postoji odluka o adekvatnoj zaštiti podataka	Može
Čl. 51 st. 1 u vezi sa čl. 54 st. 1 a)	Ustanovljavanje nadzornog organa za zaštitu podataka, koji je nadležan za nadzor primene OUZP	*Mora*
Čl. 51 st. 3 u vezi sa čl. 68 st. 4	Odredbe u u slučaju postojanja više nadzornih organa	*Mora*
Čl. 52 st. 4	Obezbeđivanje dovoljnih resursa za nadzorne organe	*Mora*
Čl. 52 st. 5	Obezbeđivanje nezavisnog personala kod nadzornog organa	*Mora*
Čl. 52 st. 6	Finansijska kontrola nadzornog organa	*Mora*
Čl. 54 st. 1 b) u vezi sa čl. 53 st. 2	Stručne predpostavke za imenovanje člana nadzornog organa	*Mora*
Čl. 54 st. 1 c) u vezi sa čl. 53 st. 1	Postupak za imenovanje člana nadzornog organa	*Mora*
Čl. 54 st. 1 d) u vezi sa čl. 53 st. 3	Trajanje mandata člana nadzornog organa	*Mora*
Čl. 54 st. 1 e)	Mogućnost ponovnog imenovanja članova nadzornog organa	*Mora*
Čl. 54 st. 1 f) u vezi sa čl. 52 st. 3, čl. 53 st. 3 i 4	Uslovi i obaveze svih članova nadzornog organa, pravila za prestanak radnog odnosa, pravila za nespojivost obavljanja određenih poslova za vreme trajanja mandata	*Mora*
Čl. 54 st. 2	Čuvanje tajnosti podataka	*Mora*
Čl. 55 st. 3 u vezi sa U.t.r. 20	Ustanovljavanje posebnih tela u okviru pravosudnog sistema država članica za obrade poda taka od strane sudova i drugih pravosudnih tela	Može
Čl. 57 st. 1 c)	Uređenje savetodavne funkcije institucije za zaštitu podataka prema parlamentu i vladi	*Mora*
Čl. 58 st. 1 f)	Postupak kontrole zaštite podataka uključujući pristup prostorijama, opremi i sredstvima obrade podataka	*Mora*
Čl. 58 st. 3 b)	Obaveza davanja mišljenja vezanih za zaštitu podataka na zahtev javnog (parlamenta, vlade itd.) ili privatnog sektora	*Mora*
Čl. 58 st. 4	Odgovarajući postupak i mogućnost postupanja po pravnom leku od strane nadzornog organa	*Mora*
Čl. 58 st. 5	Pravo tužbe i pokretanja pravnih postupaka od strane nadzornog organa	*Mora*
Čl. 58 st. 6	Dodatna ovlašćenja nadzornog organa	Može
Čl. 59	Imenovanje i drugih tela, kojima treba dostaviti izveštaj nadzornog organa	Može

Čl. 62 st. 3	Regulisanje istražnih ovlašćenja osoblja ili članova nadzornih tela iz drugih država EU	Može
Čl. 62 st. 3	Dopuštenost obavljanja istražnih ovlašćenja od strane nadzornih tela iz drugih država članica shodno pravu države članice u kojoj se vrši istraga	Može
Čl. 80 st. 1	Zastupanje pojedinaca od strane neprofitnog tela, organizacije ili udruženja	Može
Čl. 80 st. 2	Mogućnost podnošenja tužbe od strane neprofitnog tela, organizacije ili udruženja	Može
Čl. 83 st. 7	Utvrđivanje, da li će se kažnjavati tela javne vlasti i druge javne institucije	Može
Čl. 83 st. 8	Postupak za izricanje kazni, uključujući i pravne lekove	*Mora*
Čl. 83 st. 9	Posebna pravila, gde kažnjavanje ne može biti izrečeno od strane upravnog nadzornog tela	Može
Čl. 84 st. 1	Dodatne sankcije, naročito za prestupe koji nisu sankcionisani članom 83	*Mora*
Čl. 85 st. 1	Uspostavljanje saglasnosti OUZP sa osnovnim ljudskim pravom na slobodu izražavanja i informisanja, uključujući novinarske svrhe i svrhe naučnog, umetničkog ili književnog izražavanja	*Mora*
Čl. 85 st. 2	Odstupanja i izuzeci od primene OUZP za obrade u svrhe novinarstva, naučnog, umetničkog ili književnog izražavanja	*Mora*
Čl. 86	Pristup javnosti službenim dokumentima	Može
Čl. 87	Dopuštenost obrade nacionalnih identifikacionih brojeva	Može
Čl. 88	Obrada podataka u kontekstu zaposlenja	Može
Čl. 89 st. 2	Izuzeci od primene određenih prava pojedinaca pri obradi podataka u naučne ili istorijske svrhe istraživanja ili statističke svrhe	Može
Čl. 89 st. 3	Izuzeci od primene određenih prava pojedinaca pri obradi podataka u svrhe arhiviranja	Može
Čl. 90 st. 1	Regulisanje vršenja ovlašćenja nadzornih tela u skladu sa poslovnom tajnom	Može
Čl. 91 st. 2	Osnivanje posebnih nadzornih tela za crkve i religiozna udruženja ili zajednice	Može

3. DEFINICIJE

3.1. Podaci o ličnosti (čl. 4 br. 1 OUZP)

Definicija

„*Podaci o ličnosti*" su svi podaci koji se odnose na fizičko lice (u daljem tekstu pojedinca) čiji je identitet utvrđen ili se može utvrditi („*pogođeno lice*"); pojedinac čiji se identitet može utvrditi je osoba koja se može identifikovati direktno ili indirektno, naročito uz pomoć identifikatora kao što su ime, identifikacioni broj, podaci o lokaciji, identifikatori mreže ili uz pomoć jednog ili više obeležja svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

Kao što se lako iz ove definicije da zaključiti, radi se o jednoj izuzetno široko formulisanom pojmu podataka o ličnosti, koja je preuzeta iz Direktive o zaštiti podataka iz 1995. godine.

Stoga se ova definicija se shodno mišljenju ekspertske Radne grupe član 29 iz 2007. godine može svesti na 4 ključna elementa.[33]

- ✓ „*Svi podaci*" – Prema tumačenju ekspertske grupe ovaj pojam uključuje sve vrste izjava o jednoj osobi.

Pojam obuhvata *objektivne informacije* npr. postojanje određene supstance u krvi i *subjektivne informacije* kao što su npr. mišljenja i procene.

Na taj način je ovaj pojam primenljiv kod bankarskog sektora npr. da li je određeno lice poželjno da podigne kredit putem određivanja kreditne sposobnosti. Osim toga i u sektoru osiguranja da li će određeno lice ubrzo preminuti kod životnog osiguranja, pa čak i u poslovnom životu kod procene adekvatnosti radnika ili njegovog unapređenja.

U pogledu *sadržaja*, informacije mogu biti opšte i one koje se odnose na posebne kategorije podataka o ličnosti (u nauci poznate kao „osetljivi podaci").

Pojam podataka o ličnosti obuhvata i *privatni i porodični život neke osobe* u najširem smislu. Primera radi *informacije u vezi sa receptom za lekove* potpadaju u podatke o ličnosti.

Takođe ovaj pojam uključuje i *informacije o svim vrstama aktivnosti pojedinaca* npr. u vezi sa poslom, ekonomskim ili društvenim ponašanjem nezavisno od pozicije ili funkcije (potrošač, pacijent, radnik itd.).[34]

Što se tiče *formata* podataka o ličnosti on uključuje informacije u vidu teksta (abecede, azbuke), grafičke, fotografske, akustične ili druge forme.

Od izuzetnog značaja je da su obuhvaćene *papirna*, *analogna (npr. video traka) i digitalna* (elektronska, binarna forma u kompjuteru) *forma* informacija.[35]

---

[33] Radna grupa član 29, Artikel-29-Datenschutzgruppe, *Mišljenje o pojmu „podataka o ličnosti"*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE WP 136, usvojeno 20.07.2007., str. 6.

[34] *Ibidem*, str. 7.

[35] *Ibidem*, str. 8.

Fotografija kao podatak o ličnosti je regulisana u ovom pojmu, pošto su sadržane kod definicije „biometrijskih podataka“ pri obradi posebnim tehničkim sredstvima kojima se omogućava jedinstvena identifikacija ili autentifikacija pojedinca. Međutim, OUZP ih izuzima kada je u pitanju obrada posebnih kategorija podataka (U.t.r. 51 OUZP). Može se reći da OUZP tretira fotografije kao *obične podatke o ličnosti*. Na ovu kategoriju podataka trebalo primeniti opšta načela ove uredbe, zakonitost obrade, generalnu zabranu obrade ove kategorije podataka bez pristanka pojedinca. Države članice EU su upućene da u svojim zakonodavstvima regulišu ovu problematiku. Pored toga ostavljeno je državama članicama EU da posebno regulišu i tematiku *video nadzora*.

Video nadzor je shodno mišljenju ekspertske Radne grupe član 29 obuhvaćen pojmom podataka o ličnosti, ukoliko se lica mogu prepoznati sa video snimaka.

- ✓ *„O“* – Ovaj element je od odlučujućeg značaja, da bi se ustanovile međusobne veze i odnosi pojmova. Uopšteno se odnose informacije na osobu, kada se radi o *informacijama o toj osobi*.

Najčešće se u praksi informacije nedvosmisleno odnose na određeno lice.

PRIMER
Lični podaci radnika se nalaze nedvosmisleno u vezi sa njegovim radnim mestom u firmi, rezultati medicinskog testiranja su upisani u zdravstveni karton pacijenta.

Takođe postoji i puno slučajeva gde se informacije *posredno odnose na neko lice*. Tada se u prvoj liniji informacije odnose na predmete, koje su u vezi sa određenim licem.

PRIMER
Sama vrednost određene nekretnine, nije obuhvaćena pojmom podatka o ličnosti. Međutim kada se iza pojma vrednosti nekretnine dovede u vezu i njen vlasnik prilikom utvrđivanja poreza, tada se situacija menja i dolazi do ispunjenja definije podatka o ličnosti.

Osim toga informacije se mogu odnositi na *posledice određenog lica*, kada se lice na osnovu obrade podataka drugačije nego druge osobe može procenjivati.

PRIMER
Nadzor taksi vozila u cilju poboljšanja kvaliteta servisa. Ukoliko se instalira u taksi vozilo GPS sistem, koji bi omogućio određivanje lokacije tog taksi vozila u realnom vremenu. Na taj način je moguće da se mušterijama dodele najbliža vozila i uštedi gorivo. Ovom prilikom se obrađuju podaci o samom vozilu, a ne o taksi vozaču. Ne radi se dakle o proceni rada taksi vozača nego se obrada podataka vrši u svrhu optimizacije troškova. Međutim instaliranjem ovog sistema moguće je proceniti pridržavanje ograničenja brzine, pogodne trase vožnje. Stoga se lako može nadzirati i sam vozač, što može imati posledice po samog vozača. Tada bi svakako ovi podaci potpadali pod zaštitu podataka u smislu uredbe.[36]

[36] *Ibidem*, str. 14.

U praksi se često dešava da se *jedna informacija tiče više osoba*. Ovo je od izuzetnog značaja kod zahteva vezanog za pravo pristupa o obradi podataka. U tom slučaju se svaka pojedinačna osoba posebno tretira.

PRIMER
Kod pisanja protokola sa sastanka postoji lice koje je sačinilo protokol Marko, a učesnici sastanka su bili još Zoran i Ivana, koji su dali određene izjave i postupanje u budućem periodu. Zoranova izjava, da je u određeno vreme bio na određenom mestu predstavlja „podatak o ličnosti". Sama činjenica da je Marko sačinio protokol o tome da se na sednici nalazila i Ivana i njene izjave ne predstavljaju podatke o ličnosti Zorana.

- ✓ „Utvrđen identitet ili identitet koji se može utvrditi" – Sama mogućnost utvrdivosti identiteta je od značaja. Ovaj element se takođe odnosi na uske veze sa određenom osobom, koje čine *obeležje te osobe*. *Primer*: Boja kose, boja kože, visina.

U nauci se dalje u okviru ovog pojma razlikuje *direktno* ili *indirektno odredivo lice.* Tako bi direktno odredivo lice bilo – ime i prezime, a indirektno odredivo lice – IP adresa, broj socijalnog osiguranja, korisnički broj, lični broj zaposlenog u firmi, registarski broj tablica vozila, broj pasoša itd.[37]

Indirektno se može neko lice odrediti uz pomoć *kombinacije određenih njegovih obeleža*. Stoga definicija podataka o ličnosti i sadrži mogućnosti identifikovanja lica putem „imena, identifikacionih brojeva, podataka o lokaciji, identifikatora mreže ili uz pomoć jednog ili više obeležja svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca". Otvorenom klauzulom sadržanom u čl. 87 OUZP je omogućeno državama članicama EU da materiju posebnih obeležja odnosno *nacionalnih identifikacijskih brojeva* regulišu u svojim zakonodavstvima.

- ✓ „fizičko lice"- suštinski element koji određuje subjekta zaštite podataka. *Zaštita podataka se odnosi isključivo na fizička lica*. Subjekti odnosno titulari zaštite podataka su fizička lica pogođena obradom podataka.

Da je ovaj element definicije od izuzetnog značaja, pokazuju i primeri iz dosadašnje zakonodavne i sudske prakse.

PRIMER
Austrijski Zakon o zaštiti podataka (DSG 2000) je predviđao zaštitu podataka ne samo fizičkim licima nego i *pravnih lica*.[38]

[37] *Ibidem*, str. 15.

[38] Čl. 4 tč. 3 i čl. 4 i 5 austrijskog Zakona o zaštiti podataka, Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.) (CELEX-Nr.: 395L0046), https://www.ris.bka.gv.at/ GeltendeFassung.wxe? Abfrage= bundesnormen&Gesetzesnummer=10001597, 10.03.2018.

PRIMER
Nemački Ustavni sud federalne jedinice Rajna-Palatinat (nem. Rheinland-Pfalz) je dodelio *zaštitu podataka pravnim licima u vidu ustavne garancije*.[39]

PRIMER
Evropski sud je potvrdio opseg zaštite pravnih lica u okviru pojma „podaci o ličnosti“.[40] Procena zaštite ličnih podataka je drugačija za pravna lica u odnosu na fizička lica. „Pravna lica se mogu pozvati na čl. 8 Evropske karte o temeljnim pravima samo onda, kada je *ime pravnog lica određeno sa jednim ili više fizičkih lica*“.[41] Na taj način su zaštićene firme koje imaju jedno lice „Marko Marković DOO“, jer iza pojma pravnog lica treba da postoji veza sa fizičkim licem. Pošto kod ovih lica nije moguće da se napravi razlika između registrovanja kao privrednog subjekta i podataka o ličnosti, dolazi do primene zaštite podataka.

Pa ipak *OUZP isključuje ovu mogućnost* u u.t.r 14, gde se kaže da *se uredba ne odnosi* na „*pravna lica* osnovanih firmi, uključujući njihovo ime, pravnu formu i njihove kontakt podatke“. Ovome bi trebalo dodati i registarski broj firme u privrednim registrima, e-mail adresu firmi npr. info@company.com. Pored podataka vezanih za kompanije *OUZP se ne primenjuje i na anonimizovane podatke* (više o tome u nastavku poglavlje 3.2.4.).[42]

Valja podsetiti da zaštita podataka predstavlja lično, subjektivno pravo, a pre svega ljudsko pravo priznato Evropskom kartom o temeljnim pravima i Evropskom konvencijom o zaštiti ljudskih prava. Stoga je od izuzetnog značaja da su subjekti zaštite podataka isključivo fizička lica. U suprotnom bi se moglo govoriti i o zaštiti *umrlih osoba, još nerođene dece (nasciturusa), životinja*, što svakako ne potpada pod pojam definicije zaštite podataka o ličnosti.[43]

Ono što je takođe bitno istaći je da se *pravo zaštite podataka o ličnosti odnosi isključivo na žive osobe*. Umrle osobe potpadaju pod zaštitu građanskog prava, pošto se više ne mogu smatrati fizičkim licima.[44] Međutim države članice EU mogu predvideti u svojim zakonodavstvima ovu temu (U.t.r. 27 OUZP), tako da ova mogućnost predstavlja jednu „otvorenu klauzulu“.

---

[39] Presuda Ustavnog suda, broj akta B 0035/12, presuda od 13.05.2014, Der Verfassungsgerichtshof des Bundeslandes Rheinland-Pfalz , Az. B 0035/12, Urteil vom 13.05.2018.

[40] Evropski sud, broj akta C-92/09 i C-93/09, red 54, EuGH, Az. C-92/09 und C-93/09, Rz. 54, http://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=DE, 31.03.2018.

[41] *Ibidem*, str. 53.

[42] Evropska Komisija, *Šta su podaci o ličnosti*, European Commission, what is personal data, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en#examples-of-personal-data, 25.03. 2018.

[43] U pogledu začete a još nerođene dece može se možda uzeti u smislu zaštite podataka, ako bi se primenila definicija „genetskih podataka“ (videti čl. 4 tč. 13 OUZP). Ovo pitanje će sigurno biti diskutovano u praksi. Po mišljenju autora, ovaj pojam bi sa novom uredbom spadao u zaštitu podataka o ličnosti.

[44] Radna grupa član 29, Artikel-29-Datenschutzgruppe, *Mišljenje o pojmu „podataka o ličnosti“*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 01248/07/DEWP 136, usvojeno 20.07.2007., str. 25.

PRIMER
U slučaju kombinacije podataka o umrlom licu i o fizičkom licu (živom licu), podaci o određenom licu (živom licu) prilikom njihove obrade potpadaju pod zaštitu podataka o ličnosti. Podatak o tome da je umrlo lice Petar bolovalo od hemofilije i da njegov sin Ivan pati od iste bolesti.

PRIMER
Ukoliko podaci umrle osobe potpadaju pod posebnu zaštitu, koja ne stoji direktno u vezi za zaštitom podataka o ličnosti u smislu uredbe. Obaveza čuvanja tajne od strane lekara se ne završava sa smrću pacijenta. Takođe propisi iz drugih oblasti prava regulišu pravila zaštite fotografija, čuvanja časti u odnosu na umrla lica.

U najnovijoj teoriji ali i praksi se postavlja pitanje, kome pripadaju podaci odnosno *ko je vlasnik podataka „eng. Data Owner"*? Tako se često prilikom napuštanja firme, da li podaci pripadaju firmi ili radniku.

Viši sud u Nirnbergu je odlučio, da pravo raspolaganja podacima u osnovi pripada onima, koji prouzrokuju neposredno snimanje podataka. To važi i u slučaju kreiranja podataka po tuđem zahtevu u okviru radnog odnosa. Sud je dakle potvrdio pravo svojine na podacima radniku, u kome je njemu bilo povereno potpuno kreiranje podataka.[45] Tendencija ide u pravcu da se podaci odnose na onu *osobu, koja je kreirala ili proizvela podatke*. Stoga se jedna vrsta prava svojine može preneti na *„generatora" podataka*.[46] U pogledu vlasništva nad podacima sud je konstatovao: "Sa jedne strane *podaci ne predstavljaju stvari u smislu građanskog prava*, dok sa druge strane ne daju prenosni mediji i njihovo vlasništvo sam karakter pravu raspolaganja podacima, već u *snimanju podataka sadržane informacije i njihovo autorstvo*."[47]

PRIMERI I KONTROLNA LISTA PODATAKA O LIČNOSTI			
Upotreba: pravna osnova obrade podataka, prava pojedinaca i pravna osnova prenosa podataka			
Podatak o ličnosti	*Član*	*Rizik*	*Objašnjenje*
Ime, prezime (ime i prezime zajedno ili u kombinaciji sa drugim identifikatorima), nadimak	4 OUZP	Normalan	Samo ime ili samo prezime ili samo nadimak nije dovoljan parametar da bi se određena osoba identifikovala. U kombinaciji sa drugim podacima npr. datum rođenja i mesto stanovanja lice se preciznošću može identifikovati.

[45] Viši sud Nirnberg, odluka od 23.1.2013. OLG Nürnberg I. Strafsenat, Beschluss vom 23.01.2013 - I Ws 445/12 at [14].

[46] Thomas Hoeren, Big Data and the Ownership in Data: Recent Developments in Europe, European Intellectual Property Review 12/2014., S. 751 – 754, str. 753.

[47] Viši sud Nirnberg, odluka od 23.1.2013. OLG Nürnberg I. Strafsenat, Beschluss vom 23.01.2013 - I Ws 445/12 at [16].

E-mail adresa	4 OUZP	Normalan	Sa izuzetkom poslovnih e-mail adresa sa opštim obeležjima firme, uloga u firmi ili koncernu.
Adresa i poštanski broj	4 OUZP	Normalan	U kombinaciji sa imenom i prezimenom omogućava pouzdanu identifikaciju.
Poslovna adresa ili lokacija	4 OUZP	Normalan	U kombinaciji sa imenom i prezimenom omogućava pouzdanu identifikaciju.
Vreme i mesto rođenja	4 OUZP	Normalan	Koristan identifikator uz ostale parametre.
Državljanstvo	4 OUZP	Normalan	Koristan identifikator uz ostale parametre.
Izvod iz matične knjige rođenih	4 OUZP	Normalan	Dodatan parametar za identifikovanje osobe.
Pasoš ili lična karta, vozačka dozvola, putne vize	4 OUZP	*Visok*	Najčešće pasoš, lična karta, vozačka dozvola, putna viza pored skupa ličnih podataka sadrže i biometrijske podatke.
Fizička obeležja	4 st. 1 OUZP	Normalan	Opis lica, boja kože, visina, tetovaža, boja kose.
Fiziološka obeležja	4 st. 1 OUZP	Normalan	Zdravstveni karton, dijagnoza, nasledne bolesti, zarazne bolesti.
Kulturni identitet	4 OUZP	Normalan	Učešće na određenim kulturnim manifestacijama, članstvo u kulturnim organizacijama.
Socijalni identitet	4 OUZP	Normalan	Profili na društvenim mrežama, pripadnost određenoj društvenoj grupi (penzioner).
Broj socijalnog osiguranja	4 OUZP	Normalan	Broj socijalnog osiguranja nedvosmisleno služi kao ključ za zbirku podataka o nekoj ličnosti. Moguće je pratiti podatke o zaposlenosti određenog lica, uplate socialnog osiguranja i ostalih doprinosa.
Audio i video snimci i fotografije	4 OUZP	*Visok*	Svi elementi su pogodni za identifikaciju. Mogućnost za upotrebu dodatnih karakteristika kao što su glas, hod, otisak prstiju, oblik ušiju, prepoznavanje lica itd.
Broj telefona (fiksni, mobilni) uključujući broj SIM kartice i IMEI broj	4 OUZP	Normalan	Iza brojeva telefona, brojeva SIM kartice, IMEI brojeva je moguće identifikovati preplatnike ili korisnike, korisnike uređaja, lokacije uređaja ili kartica.

Identifikacioni brojevi i nalozi	4 OUZP	Normalan	Brojevi naloga kod banka, lokalnih samouprava. Identifikacioni broj zaposlenog, identifikacioni broj člana udruženja.
Podaci o lokaciji (npr. GPS)	4 OUZP	Normalan	GPS uređaji za praćenje lokacije u vozilima, mobilnim telefonima.
Evidencija izbora, odabira i pretraživanja veb sajtova	4 OUZP	Normalan	Odabrani filmovi za gledanje na Jutjubu. Izbor knjige kupljene na Amazonu. Poseta određene veb stranice, rezultati pretraživanja. Meta podaci i log fajlovi.
Nazivi fajlova i datoteka	4 OUZP	Normalan	Treba obratiti pažnu da lična imena u nazivima fajlova, datoteka i ostalih podataka mogu predstavljati podatke o ličnosti.
Digitalni potpis ili sertifikat	4 OUZP	*Visok*	Ukoliko digitalni potpis nije anoniman, onda se on tretira kao podatak o ličnosti. Zavisno od kriptografske zaštite, postoji veći ili manji rizik od krađe identiteta.
Broj PDV-a	4 OUZP	Normalan	U prvoj liniji se odnosi na samostalne preduzetnike. (taksiste, advokate, frizere itd.).
Finansijske evidencije	4 OUZP	Normalan	Štednja, penzija, akcije, obveznice, dugovi, novčane kazne, porezi.
Finansijski i bankarski podaci	4 OUZP	Normalan	Bankarski računi, broj polisa osiguranja, hipoteke, zaloge, kreditni status, istorija kredita.
Identifikatori vlasništva	4 OUZP	Normalan	Broj tablica vozila, broj garancije određenih uređaja (TV, mobilni).
Evidencija putovanja i smeštaja	PNR Direktiva 2016/681	Normalan	Rezervacije hotela, letovi, polovidbe, automatski uređaji za naplatu putarine, železnički i drumski transport, iznajmljivanje taksi vozila, rent a car, javni prevoz.
Podaci vezani za zaposlenje	4 OUZP	Normalan	Broj bankovnog računa, lični broj, zarada, CV.
Evidencije o školovanju i sertifikacijama	4 OUZP	Normalan	Svedočanstva, sertifikati, ocene, diplome, reference.

3.1.1. Podaci o ličnosti u onlajn okruženju

Specifičnost onlajn okruženja je u tome što se ovi podaci kao podaci o ličnosti ne definišu detaljno u tekstu OUZP, nego su *pomereni u uvodne tačke razmatranja*. Na ovaj način se daje tumačenje onoga, šta je zakonodavac želeo da zaštiti.

U samom čl. 4 st. 1 OUZP definicije podataka o ličnosti stoji: Svi podaci o nekoj osobi, koja se može direktno ili indirektno odrediti „naročito uz pomoć identifikatora kao što su ime, identifikacioni broj, podaci o lokaciji, identifikatori mreže".

Tako u.t.r 30 OUZP detaljno reguliše ove podatke o ličnosti:

„Pojedinci se mogu identifikovati uz pomoć identifiktora mreže kao što su IP-adrese, kolačića, koje pružaju njihovi uređaji, aplikacije, alati i protokoli, ili uz pomoć drugih identifikatora poput na primer oznaka za radiofrekvencijsku identifikaciju. Tako mogu ostati tragovi koji se, posebno u kombinaciji sa jedinstvenim identifikatorima i drugim informacijama koje primaju serviseri (provajderi), mogu upotrebiti za izradu profila pojedinaca i njihovu identifikaciju".

U pogledu *IP-adresa* postoji specifičnost, pošto se ova adresa ne može poistovetiti sa ostalim brojevima, kodovima, adresom stanovanja, registarskim brojem tablica koje su dodeljene nekom licu. IP-adresa je uporediva sa automatski dodeljenim pečatima ili kodovima dostave od strane pošte.[48]

Prema mišljenju evropskog advokata Manuela Campos Sánchez-Bordone pred Evropskim sudom u slučaju dugogodišnjeg snimanja IP-adresa od strane provajdera veb stranica u Nemačkoj, konstatovano je:

„*da podatke treba zaštititi kad je treća osoba u poziciji da konstruiše vezu kao određenoj osobi.* Nije svako znanje hipotetičke, nepoznte treće osobe relevantno. Potrebno je obratiti pažnju da li je to znanje sprovodljivo ili praktično upotrebljivo da bi moglo da pokaže dodatne informacije o vezi sa određenom osobom". [49]

Kolačići „eng. Cookies" su mali tekstualni fajlovi (tzv. podaci mrvice), koje veb sajt skladišti na računarima korisnika (tačnije u brauzerima), da bi se po potrebi brzo i pouzdano ponovo prepoznali.[50] Time su korisnici u mogućnosti da brže i pouzdanije pristupe nekom veb sajtu.[51]

---

[48] Hans G. Zeger, Was ist die IP-Adresse? - Fakten und Mythen, Argedaten, http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=25983srr, 06.03.2018.

[49] Mišljenje evropskog advokata Manuela Campos Sánchez-Bordone iz maja 2016. godine, slučaj Patrick Breyer protiv Savezne Republike Nemačke, Broj predmeta C-582/14. http://curia.europa.eu/juris/document/document.jsf?text=&docid=178241&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=795938, 10.3.2018.

[50] Najpoznatiji internet brauzeri su Internet Explorer, Google Chrome, Mozilla, Safari. Korisnici brauzera Mozilla mogu u podešavanjima isključiti opciju slanja kolačića trećim licima (npr. Fejsbuku, Guglu). Opcija se nalazi kada se u podešavanjima (tools) , pa na opcije (options) , zatim na privatnost (privacy), pa se onda pronađe prihvatanje kolačića i tu odabere opcija da se isključi trećim licima slanje kolačića - https://support.mozilla.org/sr/kb/onemogucite-kolacice-trecih-lica-kako-biste-zaustavili-pracenje-putem -reklama.

[51] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, EuroPriSe Europäisches Datenschutz-Gütesiegel, Zertifizierbarkeit von Online-Diensten zur Einblendung verhaltensbasierter Werbung („Behavioural Advertising"), 2010., str. 1.

Postoje različite vrste kolačića u zavisnosti od toga, da li se uz pomoć njih može otkriti identitet lica ili taj identitet nije moguće otkriti. Nesumnjivo je da kolačići potpadaju pod definiciju „podataka o ličnosti".

Austrijsko uduženje za zaštitu podataka Arge Daten je sastavilo vodič za primenu kolačića u praksi u zavisnosti da li je potrebna predhodna saglasnost od korisnika ili nije. Navedeni primeri su dati na osnovu još uvek važećeg zakonodavstva EU, a bazirani su na mišljenju Radne grupe član 29.

PRIMER KOLAČIĆI ZA KOJE JE NIJE NEOPHODNO PRIBAVITI PRISTANAK

- *Kolačići-kolica za kupovinu*: Kolačići čiji se sadržaj prikuplja i snima u vidu kolica za kupovinu (ikonica za to) jednog onlajn šopa ili snimanje opštih podataka o korisnicima. Ova vrsta kolačića je poznata kao *User-Input-Cookies (Session-ID).* Snimanje ovih kolačića je ograničeno na jednu posetu korisnika ili je ograničeno na određeno vreme trajanja (najčešće na nekoliko sati).
- *Sigurnosni kolačići*: Kolačići koji snimaju (protokolišu) pogrešne pokušaje pristupa sistemu (npr. pristup onlajn nalogu za kupovinu).
- *Multimedijski kolačići*: Kolačići koji služe za prikazivanje multimedijskih sadržaja. (npr. Adobe Flash). Poznatiji su i kao„*Flash-Cookies*".[52]

PRIMER KOLAČIĆI ZA KOJE JE NEOPHODNO PRIBAVITI PRISTANAK

- *Kolačići za praćenje „Tracking-Cookies"*: Kolačići koji omogućavaju analizu ponašanja korisnika u odnosu na više veb stranica.
- *Reklamni kolačići*: Kolačići koji služe u svrhu slanja reklama korisnicima.
- *Kolačići za analizu*: Kolačići koji mere broj poseta korisnika ili za procene i druge analize korisnika.

PRIMER KOLAČIĆI ZA KOJE JE USLOVNO NEOPHODNO PRIBAVITI PRISTANAK

- *Kolačići za autentifikaciju*: Kolačići za usluge kod kojih je neophodna autentifikacija za vreme trajanja jedne sesije.
  Upotreba ovih kolačića ne zahteva pribavljanje saglasnosti korisnika, sve dok je ograničena isključivo na trajanje posete jednom veb sajtu. Ukoliko se ovi kolačići koriste uz pomoć funkcije „ostani prijavljen", tada se korisnici moraju informisati o tome da će se podaci snimati i nakon trajanja posete određenom veb sajtu kao i da se saglase npr. putem checkbox-a za dalju obradu podataka.
- *Kolačići prikazivanja*: Kolačići koji snimaju informacije o prikazivanju na veb sajtu. To su npr. na kojem jeziku treba da bude prikazan određeni sajt ili da li je poželjna verzija za mobilne uređaje određenog veb sajta.
  Upotreba ovih kolačića je dopuštena na sličan način kao i kod kolačića za autentifikaciju. Ako se postavke iz brauzera snimaju duže od jedne sesije, neophodno je informisati korisnike i pribaviti njihovu saglasnost.
- *Kolačići sa društvenim dodacima „Social Plugin-Cookies"*: Kolačići koji omogućavaju deljenje sadržaja sa drugim korisnicima društvenih mreža. Korišćenje kolačića u ovu svrhu je dopušteno,ako se oni snimaju i koriste za prijavljene korisnike društvene mreže i ako omogućavaju isključivo korisnicima poželjne funkcionalnosti (lajkovanje, šerovanje itd.).[53]

[52] Radna grupa član 29, Artikel-29-Datenschutzgruppe, *Mišljenje o izuzetku obaveze pribavljanja saglasnosti kod kolačića*, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, 1676/13/DE WP 208, usvojeno 05.06.2016, Str. 7, 8.

[53] Austrijsko uduženje za zaštitu podataka Arge Daten, Vodič za primenu kolačića u praksi, Leitfaden zum datenschutzkonformen Cookie-Einsatz, http://www.argedaten.at/php-generiert/_Leitfaden_zum_datenschutzkonformen_Cookie_Einsatz.html, 31.3.2018.

Međutim ukoliko se ovi kolačići koriste za praćenje članova i onih koji nisu članovi društvenih mreža onda se mora pribaviti predhodna saglasnost.[54]

Podaci o lokaciji se odnose sa jedne strane na *boravak neke osobe na određenom području* (npr. boravak u nekom gradu, radno mesto, mesto stanovanja ili uobičajenog boravka). Sa druge strane se odnose na mogućnost izrade *profila kretanja neke osobe i druge forme profilisanja,* koje omogućavaju identifikaciju osobe uz pomoć njenog kretanja, analize ili prognoze njenog kretanja (U.t.r. 71 OUZP).

Radi se o podacima, koji se odnose na prostornu komponetu. Sadržaj ovih podataka određuje prisustvo nekog lica u određeno vreme na određenom mestu (kao i lokacija uređaja npr. pametnog telefona).

PRIMERI
-Procena lokacije zaposlenog uz pomoć GPS sistema.
-Ustanovljavanje lokacije korisnika mobilnih uređaja, na osnovu identifikacije sa baznih stanica „Cell-ID“.[55]
-Procena lokacije pametnih telefona pomoću WI-FI i preuzetih aplikacija.

Treba imati u vidu da se na nivou EU očekuju posebni propisi koji će urediti funkcinisanje u online okruženja. Za to će biti merodavna *Uredba E-privatnost* (E-Privacy Regulation), koja će biti bazirana na OUZP. Trenuto postoji nacrt uredbe, čije se usvajanje tek očekuje.[56] Početna želja Evropske Komisije je bila da ova uredba stupi na snagu zajedno sa OUZP. Međutim potpuno je jasno da do toga neće doći ni do kraja 2019. godine.

Pored analiziranih kategorija podataka (IP-adresa, kolačića i podataka o lokaciji) postoje i ostale kategorije podataka koje su merodavne za onlajn okruženje i elektronske komunikacije. One će biti prikazane u tabeli sa rezervom i napomenom u vidu posebne regulative u oblasti elektronskih komunikacija vezane za Uredbu E-privatnost.

[54] To pre svega važi za *Behavioural Advertising*, koji se odnosi na posebnu vrstu reklamiranja na internetu, kojim se surfovanje korisnika prati da bi se korisnicima pokazao određeni reklamni materijal uz pomoć banera. U zavisnosti od toga na koji reklamni sadržaj se klikne, vrši se grupacija i kategorizacija korisnika u posebne grupe na osnovu njihovih interesovanja i na taj način se dobijaju reklame. Prati internet surfovanje odnosno saobraćaj i na taj način pravi detaljno profilisanje internet korisnika. Za ovo praćenje ponašanja korisnika koriste se upravo kolačići. Andrej Diligenski, Dragan Prlja, *Fejsbuk, zaštita podataka i sudska praksa*, Institut za uporedno pravo Beograd, 2018., str. 14.

[55] Christian Bergauer, Datenschutz-Grundverordnung, Knyrim, izdato 2016., str. 54.

[56] Proposal for a Regulation of the Europan Parlament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241, 31.3.2018.

PRIMERI I KONTROLNA LISTA PODATAKA O LIČNOSTI U ONLAJN OKRUŽENJU			
Upotreba: pravna osnova obrade podataka, prava pojedinaca i pravna osnova prenosa podataka			
Podatak o ličnosti	*Član*	*Rizik*	*Objašnjenje*
Kolačići	U.t.r. 30 OUZP	Normalan	Trenutno kolačiće pored OUZP regulišu Čl. 5 st. 1 Direktive o privatnosti i elektronskim komunikacijama (Directive 2002/58/EC)[57] i čl. 5 st. 3 Direktivom kojom se menja Direktiva o privatnosti i elektronskim komunikacijama (Directive 2009/136/EC)[58]. Očekuje se donošenje E-Privacy urdedbe, koja će sveobuhvatno regulisati kolačiće.
IP-adresa	U.t.r. 30 OUZP	Normalan	Nevezano da li su statičke (nepromenljive) ili dinamičke (promenljive) IP-adrese.
RFID oznake (identifikacija putem radio frekvencije), kartice i mikročipovi kao implanti, blutut (eng. Bluetooth) mašinski čitljivi identifikacioni uređaji, kartice sa uskladištenom vrednošću (kontaktne i bezkontaktne), druge kartice povezane sa fizičkim licima (putovne kartice eng. trevel card).	U.t.r. 30 OUZP	Normalan	Svi ovi identifikatori mogu dovesti do određenog lica, kada se povežu sa onlajn zapisima.
Debitne i kreditne kartice	U.t.r. 30 OUZP	Normalan	Primena standarda PCI/DSS (eng. Payment Card Industry Data Security Standard).

[57] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002.

[58] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal L 337 , 18/12/2009.

Podatak o ličnosti	*Član*	*Rizik*	*Objašnjenje*
Mac-adrese (eng. Media Access Control Address)	U.t.r. 30 OUZP	Nizak	Pomoću mac- adrese je moguće identifikovati uređaj u lokalnoj mreži. Internet provajderi mogu identifikovati uz pomoć ostalih elemenata pouzdano korisnika. Za većinu korisnika interneta je mac-adresa nedovoljan podatak za identifikaciju. Kombinacijom mac-adrese i podataka o lokaciji moguće je doći do osobe, koja koristi određeni uređaj npr. pametni telefon.
Podaci o lokaciji	U.t.r. 71 i čl. 4 tč. 1 OUZP	*Visok*	Uz pomoć podataka o lokaciji moguće je napraviti izvršiti profilisanje pojedinca i na taj način ustanoviti njegovo kretanje, navike, ponašanje, mesto stanovanja, radno mesto, pa čak i ekonomsko stanje.

3.1.2. Slike kao podaci o ličnosti

Slike kao podaci o ličnosti predstavljaju posebnu pravnu tematiku. Specifičnost slika je u tome da li slike treba tretirati kao osetljive podatke odnosno podatke koji predstavljaju posebne kategorije podataka shodno čl. 9 OUZP? Da li se sa slika može zaključiti etničko poreklo ili rasa ili se mogu uočiti zdravstveni podaci? Kakav je tretman slika kandidata za posao ili sa slikama napravljenim u crkvi?

Neko može poći od mišljenja da fotografije treba uvek svrstati u posebne kategorije podataka npr. zdravstvene podatke (ako neko nosi naočare), podatke o etničkom poreklu (boja kože) ili politička mišljenja (demonstracije) ili verska pripadnost (fotografija u crkvi, posebna crkvena odeća). U ovom pogledu potrebno je napraviti razliku, kao i u drugim slučajevima u pravu zaštite podataka.

a) Slike kandidata za posao

Kada se radi o slikama, koje se šalju firmama od strane kandidata za posao, treba razmortriti sledeće situacije.

Činjenica da se nečije etničko poreklo ili rasa može uočiti na slici, može biti zanemariva za svrstavanje ovih podataka pod „osetljive podatke“. Sa druge strane postoji mišljenje kod nekih autora da se kod ovih slika radi o podacima, koji su ionako u „javnom prostoru“ dostupni, te se stoga dopuštenost upotrebe određuje shodno čl. 9 st. 2 e) OUZP.

Evropski sud je u jednoj odluci o video-nadzoru iz 2014. godine prosudio o dopuštenosti obrade shodno čl. 7 Direktive o zaštiti podataka. Treba primetiti da u ovoj odluci sud *nije* posmatrao podatke o ličnosti koji su prikupljeni putem *video-nadzora kao „osetljive podatke“* (u smislu čl. 8 Direktive o zaštiti podataka). Sud je u ovom slučaju

presudio da je obrada kod video-nadzora dopuštena u slučaju „pretežnijeg interesa“. Ova zakonska osnova inače ne postoji za „osetljive podatke“ u pogledu dopuštenosti obrade. Treba poći od toga da *obrada slika ne predstavlja po sebi obradu posebnih kategorija podataka*, *već zavisi od okolnosti na koji način je slika napravljena ili u koju svrhu*.

Da *slike nisu same po sebi biometrijski podaci*, govori U.t.r. 51 OUZP: „Obradu fotografija ne treba sistematski smatrati obradom posebnih kategorija podataka o ličnosti jer su one obuhvaćene definicijom biometrijskih podataka samo prilikom obrade posebnim tehničkim sredstvima koja omogućavaju jedinstvenu identifikaciju ili autentifikaciju fizičkog lica“.

Obrada slika kao standardnih (radi se uglavnom o fotografijama veličine za pasoš) u okviru postupka prijave za posao bi stoga ne bi trebalo da bude obuhvaćeno zahtevima koji se odnose na odobrenje „osetljivih podataka“ iz čl. 9 OUZP. Time ovakve slike ne bi spadale u „osetljive“ već bi dopuštenost njihove obrade određivao čl. 6 st. 1 a-f OUZP. Najčešće bi stoga dopuštenost ovakve obrade podataka bila u zaključenju ugovora, pretežnijim interesima itd.

b) Slike, koje pokazuju versku pripadnost

Ako se slike naprave iz kojih je moguće zaključiti, ko ima koju versku pripadnost, moguće je da takve slike predstavljaju „osetljive podatke“.

Kada se fotografije naprave u crkvi, tada ne postoji mogućnost da se autori pozivaju na „pretežnije interese“ kao osnov obrade podataka (shodno čl. 6 st. 1 f OUZP). Pri obradi posebnih kategorija podataka ova mogućnost ne postoji, pošto je čl. 9 st. 2 OUZP ne poznaje. Na taj način nije moguće koristiti dopuštenost obrade ovih podataka, već je *neophodno pribaviti izričitu saglasnost* (čl. 9 st. 2 a OUZP). Za pristanak mora da postoji mogućnost da se opozove i pored toga mora biti dat slobodno i tako što će pojedinac biti adekvatno informisan.

c) Verska zajednica/članovi verske zajednice

Ukoliko verska zajednica sama obrađuje sliku, onda objavljivanje fotografija nije moguće bez pristanka člana zajednice (čl. 9 st. 2 d) OUZP). Izrada fotografija bila bi dopuštena i za bivše članove ili osobe koje su u stalnom kontaktu sa zajednicom. Objavljivanje ovakvih fotografija bi takođe bilo moguće samo uz pristanak.

d) Očigledno javno dostupni podaci

Takođe postoji mogućnost da je neko lice očigledno stavilo javno svoje osetljive podatke, pa da *stoga više ta osetljivost ne postoji*. Drugim rečima da lica objavljivanjem fotografija, iako bi one trebalo da budu posebno zaštićene, samim objavljivanjem gube tu zaštitu (kao da su se lica odrekla posebne zaštite). Zato u smislu zaštite podataka ne važi čl. 9 i ne radi se o posebnim kategorijama podataka, već o „standardnim“ podacima, čija je dopuštenost obrade regulisana u čl. 6 st. 1 a-f OUZP.

Često se u praksi argumentuje dostupnost na društvenim mrežama ili uopšte na internetu ili objavljivanje fotografija u novinskim člancima. Polazi se od toga da objavljene slike, naročito pojedinaca u društvu sa ostalim pojedincima nisu dopuštene. Pritom kod fotografisanja treba obratiti pažnju na to da kod grupnih fotografija ne bude moguće, da se pojedinci identifikuju. Na taj način se umanjuje osetljivost fotografija, čak iako su načinjene u crkvi u okviru službe.

Ukoliko fotograf želi da bude siguran, preporučuje se *izričita saglasnost* osoba, koje se slikaju. U tom slučaju treba navesti svrhu korišćenja fotografije (npr. objavljivanje u novinama ili na internetu).[59]

3.2. Pseudonimizacija (čl. 4 br. 5 OUZP)

Definicija

„Pseudonimizacija" se odnosi na obradu podataka o ličnosti na način da se lični podaci više ne mogu dodeliti određenoj osobi bez upotrebe dodatnih informacija, pod uslovom da se takve dodatne informacije čuvaju odvojeno i da podležu tehničkim i organizacionim merama kako bi se osiguralo da se podaci o ličnosti ne mogu dodeliti pojedincu čiji je identitet utvrđen ili se može utvrditi.

Podatke o pseudonimima treba posmatrati kao *posredno utvrdive podatke o ličnosti*, pošto pri korišćenju pseudonima postoji mogućnost utvrđivanja identiteta osobe, koja stoji iza određenog pseudonima.[60]

I ovu kompleksnu definiciju moguće je raščlaniti na 3 bitna elementa:

1. „Lični podaci se ne mogu dodeliti određenoj osobi bez upotrebe dodatnih informacija*" – Ukoliko se neki podaci (npr. putem imena, adrese, JMBG) o određenoj osobi mogu dodeliti radi njene identifikacije, tada* ne možemo govoriti o pseudonimizaciji.
2. „Dodatne informacije se čuvaju odvojeno*" – Podaci sa kojima bi bilo moguće identifikovati određenu osobu, potrebno je čuvati odvojeno, tako da njih nije moguće spojiti. To se može postići putem organizacionog i tehničkog odvajanja podataka (npr. putem logičkog odvajanja prava pristupa podacima).* [61]

[59] Thomas Schweiger, *Fotos als senible Daten?*, https://www.dataprotect.at/2018/04/27/fotos-als-senible-daten/, 20.07.2018.

[60] Radna grupa član 29, Artikel-29-Datenschutzgruppe, *Mišljenje o pojmu „podataka o ličnosti"*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE WP 136, usvojeno 20.07.2007., str. 21.

[61] Schwartmann/Weiß, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, Leitlinie für die rechtssichere Nutzung von Pseudonimisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung, Priručnik za upotrebu rešenja vezanih za pseudonimizaciju uzimajući u obzir Opštu uredbu o zaštiti podataka, str. 10.

PREPORUKA
Pre upotrebe postupka pseudonimizacije, *treba definisati* najpre, ko ima pravo raspolaganja u vezi sa postupkom enkripcije (kriptografije) i tabelama o dodeljivanju pseudonima. Osim toga potrebno je definisati koje lice kreira pseudonime, potom da li se može isključiti rizik samog postupka pseudonimizacije i na kraju u kojim slučajevima je dopušteno spajanje podataka radi identifikacije nekog lica.

3. *„Tehničke i organizacione mere kako bi se osiguralo da se podaci o ličnosti ne mogu dodeliti pojedincu“* – Pseudonimizovani podaci *o nekoj osobi predstavljaju i dalje personalizovane podatke (odredive podatke o nekoj ličnosti) shodno OUZP, te* potpadaju pod zaštitu uredbe *(U.t.r. 26 OUZP).*

Uredba prepoznaje pseudonimizaciju pre svega kao *tehničko-organizacionu meru u cilju umanjenja rizika* (U.t.r. 28 OUZP). Pritom se primenom ove metode ne žele isključiti ostale tehničko-organizacione mere.[62]

3.2.1. Funkcije pseudonimizacije

Pseudonimizacija podrazumeva sakrivanje, ili bolje rečeno „maskiranje“ identiteta određene osobe. Na taj način ona ima *zaštitnu funkciju*.

Osim toga pseudonimizacija ima *funkciju umanjenja količine podataka*. Na taj način se ostvaruje princip minimizacije podataka (čl. 5 st. 1 c) OUZP). Pseudonimizacija predstavlja meru, kojom se sa podacima generano ophodi na štedljiv način.

Takođe sama pseudonimizacija služi i ostvarenju *principa „Privacy by design“* (čl. 25 OUZP), pošto se ovom tehničko-organizacionom merom postiže princip minimizacije podataka. U postupku *„Privacy by design“* pseudonimizacija služi razdvajanju samih podataka u najranijoj fazi pre početka obrade podataka, što direktno vodi ka delotvornoj zaštiti pojedinaca.[63]

U svrhu *bezbedne obrade podataka o ličnosti*, pseudonimizacija može biti upotrebljena kao tehničko-organizaciona mera (U.t.r. 83 OUZP). A predviđena je kao poželjna mera za bezbednost podataka izričito u čl. 32 st. 1 a) OUZP.

Pored toga funkcija pseudonimizacije u *smanjenju rizika po pogođene osobe* (U.t.r. 75 OUZP). Tako ova mera može dovesti do umanjenja rizika od materijalne štete (npr. od krađe identiteta, prevara, finansijskih gubitaka) ili nematerijalne štete (npr. povrede ugleda odgovornog lica).[64]

Mera pseudonimizacije *može* dovesti i do *izostanka obaveze informisanja pojedinaca pri povredi bezbednosti podataka* (čl. 34 OUZP). Tada je potrebno

[62] *Ibidem*, str. 11.

[63] *Ibidem*, str. 14.

[64] *Ibidem*, str. 15.

napraviti procenu rizika i ustanoviti, da li postoji visok rizik po prava pojedinca, čak i ako su sami podaci pseudonomizovani.[65]

PRIMER
Ukoliko dođe do krađe podataka, koji su pseudonomizovani, tada u većini slučajeva ne bi bilo više moguće identifikovati pojedince. Stoga bi nestala i obaveza informisanja pojedinaca iz čl. 34 OUZP.

3.2.2. Upotreba pseudonimizacije

Pseudonimizaciju se može upotrebljavati u *svrhu arhiviranja u javnom interesu, statističke svrhe i u svrhe naučnog ili istorijskog istraživanja*.[66] Tako čl. 5 st. 1 b) OUZP reguliše *mogućnost daljeg korišćenja podataka* u pomenute svrhe, kao izuzetak od vezanosti za prvobitnu svrhu obrade podataka: „dalja obrada u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, u skladu sa članom 89. stavom 1. ne smatra se neusklađenom sa prvobitnim svrhama („ograničavanje svrhe")".

Ova mogućnost daljeg korišćenja podataka u svrhu arhiviranja u javnom interesu, statističke svrhe i u svrhe naučnog ili istorijskog istraživanja *uslovljena je upotrebom odgovarjućih tehničko-organizacionih mera. Kao jedna od odgovarajućih mera* se navodi upravo *pseudonimizacija* (čl 89 st. 1 OUZP).

U eri upotrebe *Big Data* i *Internet of Things*, sama pseudonimizacija može doprineti zakonitosti obrade podataka u ove svrhe.

Tako čl. 6 st. 4 e) OUZP izričito reguliše *mogućnost korišćenja podataka, koji nisu prikupljeni sa istom svrhom ili za koje ne postoji pristanak*, ako se koristi pseudonimizacija.

„Ako se obrada u svrhu koja je različita od svrhe u koju su podaci prikupljeni ne temelji na pristanku pojedinca ili na pravu Unije ili pravu države članice koje predstavlja nužnu i proporcionalnu meru u demokratskom društvu za zaštitu ciljeva iz člana 23. stav 1., rukovalac*, sa ciljem utvrđivanja da li je obrada u drugu svrhu u skladu sa svrhom za koju su lični podaci prvobitno prikupljeni, uzima u obzir*, između ostalog:

(e) postojanje odgovarajućih zaštitnih mera, koje mogu uključivati enkripciju ili *pseudonimizaciju*.".

Pseudonimizacija po pravilu nije sama odlučujuća za zakonitu dalju obradu podataka, pošto je potrebno proveriti i sve ostale kriterijume iz čl. 6 OUZP. Ipak *bi se moglo reći pri proceni kriterijuma iz čl. 6 st. 4 OUZP* vezanih za dalju obradu podataka, da je sama *dalja obrada podataka dopuštena uz korišćenje pseudonimizacije*.[67]

[65] *Ibidem*, str. 26, 27.

[66] Radna grupa član 29, Artikel-29-Datenschutzgruppe, *Mišljenje o pojmu „podataka o ličnosti"*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, WP 136, usvojeno 20.07.2007., str. 21.

[67] Schwartmann/Weiß, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, *Leitlinie für die rechtssichere Nutzung von Pseudonimisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung*, Priručnik za upotrebu rešenja vezanih za pseudonimizaciju uzimajući u obzir Opštu uredbu o zaštiti podataka, str. 16.

Upotreba pseudonimizacije može se smatrati kao *legitiman interes obrade podataka i u slučaju procene pretežnijeg interesa.*

Još jedna od mogućnosti zakonitosti obrade podataka određena je čl. 6 st. 1 f) OUZP „obrada je nužna *za potrebe pretežnijih legitimnih interesa rukovaoca obrade* (odgovornog lica) ili treće strane, osim kada su od tih interesa jači interesi ili osnovna prava i slobode pojedinaca, koji zahtevaju zaštitu ličnih podataka, naročito ako je pojedinac (pogođeno lice) dete".

Procenom legitimnog interesa rukovaoca u obradi podataka u odnosu na prava prava pojedinaca, moglo bi se reći da *interesi rukovaoca (odgovornog lica) pretežu u odnosu na prava pojedinaca*, *ukoliko je rukovaoc koristio pseudonimizaciju*.[68]

Pseudonimizacija može dovesti i do toga da *rukovalac (odgovorno lice) osobodi velikog broja obaveza prema pojedincima* kao što su: prava pojedinca na informacije o obradi podataka, prava na ispravku podataka, prava na brisanje podataka „prava na zaborav", prava na ograničenje obrade podataka, prava na izveštavanje u vezi sa ispravkom ili brisanjem ili ograničenjem obrade podataka, prava na prenosivost podataka (čl. 15-20 OUZP).

Ovo pravo rukovaoca proizlazi iz člana 11 st. 1 i 2 OUZP. Ako za obradu podataka rukovaoca nije neophodna ili nije više neophodna identifikacija pojedinca, rukovalac nije u obavezi da čuva, prikuplja ili obrađuje dodatne informacije radi identifikovanja pojedinaca, a samo u svrhu ispunjenja OUZP. Stoga rukovalac nije u mogućnosti da ispuni prava pojedinaca (čl. 15-20 OUZP), a kao *dokaz* za to može poslužiti pseudonimizacija (čl. 11 st. 2 OUZP).[69]

Može se zaključiti da *i dalje postoje obaveze za rukovaoce iz čl. 21 i 22 OUZP*.

Pravo na prigovor iz čl. 21 OUZP može uložiti pojedinac:

- ✓ Ako se radi o obradi podataka, koja je nužna za izvršavanje obaveza od javnog interesa ili pri vršenju javne vlasti od strane rukovaoca (čl. 6 st. 1 e) OUZP)
- ✓ Pri obradi podataka na osnovu prezežnijeg legitimnog interesa (čl. 6 st. 1 (f) OUZP), uključujući izradu profila.
- ✓ Obrada podataka u naučne ili istorijske istraživačke svrhe kao i u statističke svrhe (čl. 89 st. 1 u vezi sa čl. 21 st. 6 OUZP).
- ✓ Obrada podataka u svrhu direktnog marketinga (čl. 21 st. 2 OUZP).

Pravo pojedinca na nepodvrgavanje automatskoj obradi podataka uključujući profilisanje (čl. 22 OUZP): Mera pseudonimizacije takođe ne isključuje ni ovo pravo pojedinca.

---

[68] Kühling/Buchner, *DS-GVO*, Art.6, Rn 156.

[69] Schwartmann/Weiß, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, *Leitlinie für die rechtssichere Nutzung von Pseudonimisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung*, Priručnik za upotrebu rešenja vezanih za pseudonimizaciju uzimajući u obzir Opštu uredbu o zaštiti podataka, str. 16.

3.2.3. Pseudonomizovani podaci i obaveza informisanja pojedinaca

Posebnosti podataka koji su pseudonomizovani pri ispunjenju obaveze informisanja pojedinaca odgledaju se u:

- ✓ Obavezi informisanja pojedinaca postoji *u trenutku prikupljanja podataka* (čl. 13 st. 1 i 2 OUZP). U ovom momentu *ne smeju podaci još uvek biti pseudonomizovani*, da bi se mogla ostvariti obaveza informisanja pojedinaca.
- ✓ Obavezi informisanja pojedinca, *kada podaci nisu prikupljeni od pojedinca*, postoji slučaj gde podaci ne smeju biti pseudonomizovani (čl. 14 st. 3 b) OUZP). U pitanju je slučaj *kada se podaci o ličnosti koriste za komunikaciju sa pojedincem* (npr. direktni marketing).
- ✓ Obavezi informisanja pojedinaca u *slučajevima dalje obrade podataka u drugu svrhu koja je različita od one za koju su podaci o ličnosti prikupljeni*, nevezano za to da li su podaci prikupljeni od pojedinca ili nisu prikupljeni od pojedinca (čl. 13 st. 3 i čl. 14 st. 4 OUZP).

PRIMER
Ukoliko rukovalac pre nameravane obrade podataka u drugu svrhu izvrši postupak pseudonimizacije, primalac (treće lice, odnosno novi rukovalac) neće biti u mogućnosti da bez dodatnih informacija identifikuje pojedinca. Stoga se savetuje da novi rukovalac na svojoj veb stranici objavi, da se obrađuju pseudonimizovani podaci. Informacije iz čl. 13 i čl. 14 OUZP se ne moraju individualno plasirati, već je moguće to izraziti putem veb sajta ili u ugovorima.

3.2.4. Anonimizacija

Anonimizacija nije direktno definisana u tekstu uredbe, već je takođe njeno objašnjenje dato u U.t.r. 26 OUZP „Načela zaštite podataka stoga se *ne bi trebala primjenjivati na anonimne informacije*, odnosno informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, ili *na lične podatke koji su anonimimizovani na način da se identitet pojedinca ne može ili više ne može utvrditi*. Ova uredba se stoga ne odnosi na obradu takvih anonimnih informacija, između ostalog na statističke ili istraživačke svrhe“.[70]

Od izuzetnog značaja je razumeti i samu razliku između anonimizacije i pseudonimizacije. U tom kontekstu je do sada bilo u praksi sporno, *kada nastupa stanje, da se određena osoba više ne može identifikovati*. Odgovor na ovo pitanje takođe dat je u U.t.r. 26 OUZP „ Da bi se odredilo može li se identitet pojedinca utvrditi, trebalo bi uzeti u obzir *sva sredstva*, poput primera radi *selekcije*, koju *rukovalac (odgovorno lice) ili*

[70] *Ibidem*, str. 12.

bilo koja druga osoba mogu po opštoj proceni verovatno upotrebiti u svrhu direktnog ili indirektnog utvrđivanja identiteta pojedinca. Da bi se utvrdilo, da li se po opštoj proceni sredstvo verovatno može upotrebiti za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir *sve objektivne faktore*, kao što su *troškovi i vreme* potrebno za utvrđivanje identiteta, uzimajući u obzir i *tehnologiju dostupnu u vreme obrade i tehnološki razvoj*".

Odlučujući elementi su:

- ✓ Troškovi identifikacije
- ✓ Potrebno vreme za identifikaciju
- ✓ Dostupnost tehnologije u vreme obrade
- ✓ Tehnološki razvoj
- ✓ Ostali objektivni faktori

Da bi se govorilo o anonimizaciji u smislu uredbe, potrebno je da postoji jedno *stanje verovatnoće u* određenom *trenutku* (ne za sva vremena!!!), da zbog teškoća u vidu vremena, troškova i ostalih faktora *je teško moguće do nemoguće*, doći do utvrđivanja identiteta osobe.[71]

Pseudonimizovani podaci
Pojedinac se može uz pomoć odvojeno čuvanih podataka ili javno dostupnih informacija ponovo identifikovati

≠

Anonimizovani podaci
Pojedinac se ne može identifikovati ili se može identifikovati samo uz ogromne napore

3.2.5. Primeri pseudonimizacije i anonimizacije

Primer pseudonimizacija

Ime	*Pseudonim*	*Posao*	*Pol*	*Datum rođenja*	*Predmet*	*Škola*
Petar Petrović	4711	Učitelj	M	12.12.1980	Matematika	Matematička gimnazija
Mina Nikolić	5566	Učiteljica	Ž	07.08.1965	Engleski	Filološka gimnazija
Uroš Jovanović	Xyz2312	Učitelj	M	04.06.1971	Biologija	Gimnazija
Mila Stevanović	JKLTZTZ	Učiteljica	Ž	02.02.1989	Srpski i muzičko	Osnovna škola

[71] *Ibidem*, str. 13.

Razlika kod pseudonimizacije u odnosu na anonimizaciju je ta da je identifikacija lica moguća. Odnos podataka o ličnosti i pseudonima se uspostavlja uz pomoć *referenci*, koje se pojedinačno određuju za svako lice. Dopuštenost povratka informacija uz pomoću referenci treba da bude određen od strane rukovaoca ili zakonodavca. Zaposleni koji obrađuje pseudonimizovane podatke ne sme imati pristup referencama.

Pseudonim	*Posao*	*Pol*	*Predmet*	*Škola*
5744	Učitelj	m	Matematika	Matematička gimnazija
8866	Učiteljica	ž	Engleski	Filološka gimnazija
Xyz1452	Učitelj	m	Biologija	Gimnazija
JKLTWGJ	Učiteljica	ž	Srpski i muzičko	Osnovna škola

U praksi pseudonimizaciju treba koristiti pre svega, kada se želi istraživati u dužem periodu život ili ponašanje osoba. Može se desiti da je korišćenje podataka bez njihove veze sa određenim osobama dovoljno da bi se postigao određeni cilj. Jedna takva situacija bi bila kada bi podaci od školskog lekara bili poslati nekom naučnom institutu radi procene bolesti dece. Tom prilikom ne bi bilo moguće identifikovati decu. U ovom slučaju bi lista referenci vezanih za pseudonime bila kod nadležnog Ministarstva zdravlja.

Primer anonimizacija

Ime	*Posao*	*Pol*	*Datum rođenja*	*Predmet*	*Škola*
Petar Petrović	Učitelj	m	12.12.1980	Matematika i fizičko	Matematička gimnazija
Mina Nikolić	Učiteljica	ž	07.08.1965	Engleski	Filološka gimnazija
Uroš Jovanović	Učitelj	m	04.06.1971	Biologija	Gimnazija
Mila Stevanović	Učiteljica	ž	02.02.1989	Srpski i muzičko	Osnovna škola

Pod anonimizacijom se podrazumeva da se pojedinac ne može uopšte ili samo uz izuzetne napore identifikovati. Za anonimizaciju je od značaja da se *ime i datum rođenja odstrane*, tako da identifikacija lica više ne bi bila moguća. Na ovom primeru bi ipak bilo neophodno da se dobiju ostale informacije, da bi se osoba mogla identifikovati uz pomoć predmeta, pola i škole.[72]

[72] Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, *Was versteht man unter Datenverarbeitung?,* https://www.datenschutzzentrum.de/artikel/1091-Was-versteht-man-unter-Datenverarbeitung.html, 20.6.2018.

Ime	*Posao*	*Pol*	*Datum rođenja*	*Predmet*	*Škola*
	Učitelj	m		Matematika i fizičko	Matematička gimnazija
	Učiteljica	ž		Engleski	Filološka gimnazija
	Učitelj	m		Biologija	Gimnazija
	Učiteljica	ž		Srpski i muzičko	Osnovna škola

3.3. Posebne kategorije podataka o ličnosti (čl. 9 OUZP)

U ovom poglavlju biće razmatrane ključne kategorije posebnih podataka o ličnosti. Za ove kategorije podataka se uobičajen naziv u praksi „*osetljivi podaci*“ o ličnosti (U.t.r. 10 OUZP).

U okviru definicije osetljivih podataka nalaze se sledeće kategorije podataka o ličnosti:

- ✓ Podaci o rasnom ili etničkom poreklu;
- ✓ Podaci o političkom mišljenju;
- ✓ Podaci o verskom ili filozofskom uverenju;
- ✓ Podaci o članstvu u sindikatima;
- ✓ Genetski podaci;
- ✓ Biometrijski podaci;
- ✓ Zdravstveni podaci;
- ✓ Podaci o polnom životu ili seksualnoj orijentaciji.

OUZP definiše samo genetske, biometrijske i zdravstvene podatke. Stoga će njima biti posvećena posebna pažnja.

3.3.1. Genetski podaci (čl. 4 br. 13 OUZP)

Definicija

„Genetski podaci” su podaci o ličnosti, koji se odnose na nasleđena ili stečena genetska obeležja pojedinca, koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, naročito ako su dobijeni analizom biološkog uzorka dotičnog pojedinca.

Ova definicija dopunjena je i proširena u U.t.r. 34 OUZP.

„Genetske podatke bi trebalo definisati kao podatke o ličnosti u vezi sa nasleđenim ili stečenim genetskim obeležjima pojedinca, koji proizlaze iz analize biološkog uzorka pojedinca o kojem je riječ, naročito analize hromozoma,

dezoksiribonukleinske kiseline (DNK) ili ribonukleinske kiseline (RNK) ili iz analize drugog elementa, koji omogućuje dobijanje jednakovredne informacije".

PRIMER GENETSKA OBELEŽJA
Nasledne genetske bolesti (hemofilija, daltonizam, daunov sindrom ...), genetski faktori koji utiču na razvoj čoveka (kloniranje, vantelesna oplodnja itd.).

Iako je do sada u literaturi DNK analiza odnosno analiza gena spadala u biometrijske podatke, može se primetiti da su zbog značaja i izuzetne osetljivosti u praksi DNK odnosno genetski podaci postali nova *posebna kategorija podataka o ličnosti* (čl. 9 st. 1 OUZP).

PRIMER UPOTREBE GENETSKE ANALIZE
Analiza gena se danas koristi u prevenciji od oboljevanja po osnovu raznih bolesti.
Kardiologija: Koronarna bolest srca, infarkt miokarda, aneurizma, hipertenzija, stabilnost pritiska, tromboza.
Ishrana: Dislipidemija, ateroskleroza, gojaznost, dijabetes, insulinska rezistencija, vitaminski metabolizam, netolerancija na laktozu, tolerancija alkohola.
Rak: digestivni trakt, pluća, grudi, prostata, supresorski gen tumora.
Centralni nervni sistem: depresija, burnout, stres, vaskularna demencija, Alchajmerova bolest, moždani udar, zavisnost od spoljnih uticaja.
Detoksikacija: Obimna analiza enzima faza I II.
Farmakogenetika: Obimna analiza metabolizma lekova uljučujući CYP2D6, CYP2C9, CYP2C19, CYP1A2, QT-vreme, SLCO1B1 (statin), COMT, MAOA, ITGB (osetljivost na aspirin) i terapije zamene hormona.
Ostale bolesti: Osteoporoza, molekularna deneracija vezana za starost, receptor vitamina D.[73]

Osim toga ukoliko primetimo kategoriju fizioloških karakteristika kod biometrijskih podataka, može se zaključiti da je dobar deo ovih karakteristika genetski determinisan (mustre vena, znojne pore, miris tela, prepoznavanje glasa itd.). Stoga će u praksi biti od velike važnosti napraviti *razgraničenje*, kada su u pitanju kategorije *biometrijskih i genetskih podataka*. Može reći da je razlika između genetskih podataka i biometrijskih u tome što *genetski podaci zahtevaju identifikaciju lica u pogledu njegovog zdravlja ili fiziologije putem genetskih obeležja*. Sa druge strane *biometrijski podaci služe isključivo identifikaciji* određene osobe, između ostalog i *putem genetskih obeležja materijala DNK*.

Za genetske podatke je takođe predviđena *otvorena klauzula*, tako da države članice EU mogu zadržati ili uvesti dodatne uslove ili ograničenja u pogledu ove kategorije podataka (čl. 9 st. 4 OUZP).

[73] Primeri genetske analize, was ist eine genanalyse und warum kann sie leben retten?, https://www.matthai.at/index.php/Genanalyse.html, 20.5.2018.

Iz definicije genetskih podataka OUZP proizlazi da genetska obeležja pojedinca *moraju nedvosmisleno potvrditi fiziologiju ili zdravlje tog pojedinca*.

PRIMER
Ukoliko postoji određeni DNK materijal, a ne zna se kome pripada, može se reći da u tom slučaju ne potpada taj geneski materijal pod zaštitu OUZP. Potrebno je da se iz DNK materijala može zaključiti pouzdano da se radi o određenom licu, koje boluje npr. od hemofilije (zdravstveno stanje određenog lica). Tada se može reći da se radi o genetskim podacima u smislu OUZP.

3.3.2. Biometrijski podaci (čl. 4 br. 14 OUZP)

Definicija

„Biometrijski podaci" su podaci o ličnosti dobijeni posebnom tehničkom obradom u vezi sa fizičkim obeležjima, fiziološkim obeležjima ili obeležjima ponašanja pojedinca, koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci.

Najpre treba konstatovati da biometrijske podatke OUZP tretira kao *posebnu kategoriju podataka o ličnosti* (čl. 9 st. 1 OUZP). Predviđena je i *otvorena klauzula*, tako da države članice EU mogu zadržati ili uvesti dodatne uslove ili ograničenja u pogledu ove kategorije podataka (čl. 9 st. 4 OUZP).

PRIMER FIZIČKA OBELEŽJA
Otisak prsta, prepoznavanje lica, prepoznavanje dužice očiju, oblik ušiju, oblik ruku itd.

PRIMER FIZIOLOŠKA OBELEŽJA
Analiza mustra vena, analiza znojnih pora, analiza mirisa tela, prepoznavanje glasa, analiza DNK mustra itd.[74]

PRIMER OBELEŽJA PONAŠANJA POJEDINCA
Identifikacija potpisa, analiza kucanja po tastaturi, analiza hoda itd.[75]

Iz definicije biometrijskih podataka OUZP proizlazi da ponašanje kao obeležje ili fizička obeležja ili fiziološka *obeležja nekog pojedinca moraju nedvosmisleno potvrditi identitet tog pojedinca*.

[74] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Radni papir o biometriji*, Arbeitspapier über Biometrie, WP 80, 12168/02/DE, usvojeno 01.08.2003., str. 3.

[75] *Ibidem*, str. 4.

PRIMER
Ukoliko rukovalac prikuplja potpise kao obeležje neke osobe, a nije u mogućnosti da ustanovi na osnovu potpisa, koje lice tačno stoji iza određenog potpisa. Tada potpis kao obeležje nekog lica ne predstavlja biometrijski podatak u smislu OUZP, pošto ne vodi do identifikacije te osobe. Tada je potrebno zapitati se da li je prikupljanje biometrijskih obeležja neophodno i da li služi svrsi prikupljanja ovih podataka, kao i da li uopšte postoji zakonita obrada podataka. Sam potpis kao obeležje nekog lica predstavlja podatak o ličnosti, nevezano za to da li nedvosmisleno vodi ka identitetu određene osobe i stoga potpada pod zaštitu OUZP.

Prema mišljenju ekspertske Radne grupe član 29 iz 2012. godine „biometrijski podaci nepovratno menjaju *odnos između tela i identiteta*, jer oni čine *karakteristike ljudskog tela mašinski čitljivim* i *predmetom dalje upotrebe*“.[76]

Ovi podaci se uglavnom koriste za identifikaciju *prilikom kontrole pristupa* radi potvrde identiteta određene osobe. *U forenzici* se biometrijski podaci koriste u svrhu nedvosmislenog utvrđivanja identiteta neke osobe.

Da bi se govorilo o biometrijskim podacima u tehničkom smislu potrebno je imati:

- ✓ *Šablon* u običnom formatu (npr. slika)
- ✓ *Algoritam* za procenu (npr. lica), koji specifične karakteristike traženog objekta (npr. lica) izvlači i procenjuje, da bi se dobio
- ✓ *Biometrijski šablon* (eng. template), koji služi za specifično prepoznavanje određenog lica.[77]

3.3.3. Zdravstveni podaci (čl. 4 br. 15 OUZP)

Definicija

„*Zdravstveni podaci”* su podaci o ličnosti, koji se odnose na fizičko ili mentalno zdravlje pojedinca, uključujući pružanje zdravstvenih usluga, iz kojih proizlaze informacije o njegovom zdravstvenom statusu.

U zdravstvene podatke spadaju mnogobrojne informacije o pojedincima, koje će biti date kroz primere.

---

[76] Radna grupa član 29, Article 29 Data Protection Working Party, *Mišljenje o razvoju biometrijskih tehnologija*, Opinion 3/2012 on developments in biometric technologies, WP 193, 00720/12/EN, usvojeno 27.04.2012., str. 4.

[77] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Radni papir o biometriji*, Arbeitspapier über Biometrie, WP 80, 12168/02/DE, usvojeno 0108.2003., str. 4.

PRIMER ZDRAVSTVENI PODACI
- Podaci koji se odnose na fizičko ili mentalno zdravlje: informacije o bolesti, invaliditetu, rizicima bolesti, istoriji bolesti, kliničkom lečenju, fiziološkom ili biomedicinskom stanju. - Podaci koji se odnose na usluge lečenja: informacije vezane za brojeve, simbole ili obeležja koja su dodeljena određenoj osobi radi identifikacije. Informacije o ispitivanju ili lečenju delova tela. Informacije dobijene na osnovu slika kao npr. rendgena, kompjuterske mamografije, magnetne rezonance o stanju jedne osobe. - Opšti zdravstveni podaci: da li je neka osoba slomila nogu, da li neka osoba nosi naočare ili sočiva, podaci o emocionalnoj i intelektualnoj sposobnosti (npr. IQ), informacije o pušenju, o tome koliko neka osoba pije ili o drugim navikama, podaci o alergijama otkriveni javnim institucijama (npr. školama, bolnicama) ili privatnom sektoru (npr. osiguranje), članstva pojedinaca u zdravstvenim udruženjima za podršku pacijentima (npr. grupa za podršku pacijentima koji su oboleli od raka), samo pominjanje da li je neko bolestan u kontekstu rada.[78] - Zdravstveni podaci u vezi sa pametnim uređajima (eng. Wearables): merenje pulsa, krvnog pritiska uz pomoć aplikacija vezanih za zdravlje (Health-App) i fitnes aplikacija (Fitness-App).

U praksi se često postavlja pitanje, kada postoje zdravstveni podaci? Da ovo pitanje nije beznačajno i da je potrebno pravilno ustanoviti, da li se radi o zdravstvenim podacima pokazaće sledeći primer.

Da li postoje zdravstveni podaci?			
Kombinovana obrada podataka	Visina	težina	pušač

Odgovor na ovo pitanje proizlazi iz gore navedene definicije zdravstvenih podataka. U ovom slučaju je bitan deo definicije gde se kaže da se radi o zdravstvenim podacima ukoliko se *mogu izvesti informacije o zdravstvenom statusu pojedinca*.

Osim toga u U.t.r. 35 OUZP kaže se: Podaci o ličnosti, koji se odnose na zdravlje trebali bi obuhvatati *sve podatke* koji se odnose na zdravstveno stanje pojedinca, a koji otkrivaju informacije u vezi sa ranijim, trenutnim ili budućim fizičkim ili mentalnim zdravstvenim stanjem pojedinca.

Pritom se ne radi o svakoj teoretskoj mogućnosti da podaci mogu dovesti do podataka o zdravstvenom stanju pojedinca, već *treba da postoji dovoljna sigurnost* da se se do tih podataka može doći.[79]

Pa ipak se ne radi se samo o proceni toga, da li se određene informacije mogu izvesti o zdravstvenom stanju pojedinca, već koji podaci se uopšte mogu definisati kao zdravstveni. Radna grupa član 29 je u svom mišljenju iz 05.02.2015. godine proširila i pojasnila pojam definicije zdravstvenih podataka. Zdravstveni podaci postoje ako su:

- ✓ Podaci u osnovi / jasno zdravstveni podaci;
- ✓ Podaci, sirovi podaci senzora koji se mogu koristiti sami po sebi ili u

[78] Radna grupa član 29, Article 29 Working Party, *Aneks – zdravstveni podaci u aplikacijama i uređajima*, ANNEX - health data in apps and devices, str. 2 https://perma.cc/6FAS-GY6F, 30.3.2018.

[79] Dietmar Jahnel, Handbuch Datenschutzrecht, Jan Sramek Verlag, 2010., Rz 3/90.

kombinaciji sa drugim podacima, kako bi se izvukli zaključci o stvarnom zdravstvenom stanju ili zdravstvenom riziku osobe;

- ✓ Utvrđeni zaključci o zdravstvenom stanju ili zdravstvenom riziku osobe (bez obzira da li su ti zaključci tačni ili netačni, legitimni ili nelegitimni, ili na drugi način adekvatni ili neadekvatni).[80]

Da li postoje zdravstveni podaci?			
Primer	*Sektor osiguranja*		*Životno osiguranje*
Kombinovana obrada podataka	Visina	težina	pušač
	175cm	120kg	
Svrha	Procena rizika po zdravstveno stanje (potencijalnog) osiguranika	Procena rizika po zdravstveno stanje (potencijalnog) osiguranika	Procena rizika po zdravstveno stanje (potencijalnog) osiguranika
Rešenje	U kombinaciji sa podacima težina i pušač predstavljaju zdravstveni podatak, pošto se može izvesti rizik po zdravlje pojedinca (nezavisno od toga da li rizik postoji ili ne)	U kombinaciji sa podacima visina i pušač predstavljaju zdravstveni podatak, pošto se može izvesti rizik po zdravlje pojedinca (nezavisno od toga da li rizik postoji ili ne)	U osnovi zdravstveni podatak

Pored konstatacije na ovom primeru da se radi o zdravstvenim podacima, potrebno je ustanoviti i *u koju svrhu su ovi podaci prikupljeni*. Može se reći da je u ovom kontekstu odlučujuća svrha, da bi se ustanovilo da li se radi o obradi zdravstvenih podataka. Moguće je da se obrađuju i samo kategorije visina i težina, pa je iz toga može zaključiti da možda neko ima problem sa zdravljem. Na taj način bismo govorili o obradi zdravstvenih podataka.

Ukoliko su pak zdravstveni podaci prikupljeni u statističke svrhe, tada svakako ne bi bilo reči o obradi zdravstvenih podataka. U ovom slučaju je neophodno preduzeti odgovarajuće zaštitne mere (čl. 89 st. 1 OUZP). Lako je zaključiti da *sama definicija zdravstvenih podataka kao takvih ne opredeljuje konačnu obradu podataka*. Stoga bi prikupljanje zdravstvenih podataka u svrhu statistike potpadalo pod tretman člana 89 OUZP (videti izuzetak od primene čl. 9 st. 2 slovo j) OUZP).

3.4. Profilisanje (čl. 4 br. 4 OUZP)

Danas je profilisanje i automatsko donošenje odluka u upotrebi i u privatnom i u javnom sektoru. Ove tehnike i tehnologije se primenjuju u bankarstvu i finansijama,

[80] Radna grupa član 29, Article 29 Working Party, Aneks – zdravstveni podaci u aplikacijama i uređajima, ANNEX - health data in apps and devices, str. 4, https://perma.cc/6FAS-GY6F, 30.03.2018.

zdravstvu, obrazovanju, za oporezivanje, poslovima osiguranja, marketinga i oglašavanja.

Konceptom Big Data i sposobnošću analiziranja velike količine podataka, veštačke inteligencije i drugih metoda izrade profila i automatskog donošenje odluka, došlo je do povećanja uticaja i rizika po prava i slobode pojedinaca. Velika količina podataka na internetu i podataka sa uređaja za internet stvari (IoT) sposobnost pronalaženja korelacija i povezivanja podataka, omogućava lako utvrđivanje, analiziranje i predviđanje ličnih aspekata ili ponašanja pojedinaca kao i njihovih interesovanja i navika.

Samo profilisanje i automatsko donošenje odluka predstavljaju velike prednosti za organizacije pre svega u cilju povećanja efikasnosti i uštede resursa. Profilisanje i automatsko donošenje odluka se koristiti za bolje procenjivanje tržišta i prilagođavanje usluga i proizvoda potrebama pojedinaca.

U pogledu zaštite podataka, izradom profila i automatskim donošenjem odluka postoji *velika verovatnoća nastupanja rizika* za prava i slobode pojedinaca. Zbog toga je neophodno primeniti odgovarajuće mere zaštite. Najčešće se ovakvi postupci obrade odvijaju bez znanja i svesti pojedinaca da se o njima izrađuju profili. Osim toga i ako postoje informacije pojedinci velikom broju slučajeva ne razumeju same postupke. Uz sve to ovi postupci pošto se odvijaju bez znanja i svesti pojedinaca krše načelo transparentnosti (čl. 5 st. 1 a) OUZP).

Izrada profila može na pojedinca imati uticaj u vidu *stereotipa i odvojenosti društva*. Sam postupak razvrstavanja pojedinaca u određene kategorije, može im *ograničiti izbor* (npr. određenog proizvoda ili usluga), *na osnovu njihovih preferencija*. Štaviše, profilisanje može dovesti do *pogrešnih prognoza i predviđanja*, a *u krajnjoj liniji do uskaćivanja usluga ili roba, kao i do diskriminacije*.

OUZP osigurava da se profilisanje i automatsko donošenje pojedinačnih odluka ne koriste na način koji bi imao negativan uticaj na prava pojedinaca. Ovi zahtevi se odnose na:

- ✓ posebne zahteve u pogledu transparentnosti i poštenja,
- ✓ proširene obaveze u pogledu odgovornosti,
- ✓ posebno navedene pravne osnove za obradu,
- ✓ prava pojedinaca da izraze prigovor izradi profila, a naročito profilisanju u marketinške svrhe,
- ✓ pod određenim uslovima, neophodnost sprovođenja procene uticaja u vezi sa zaštitom podataka.

OUZP nalazi primenu ne samo na odluke donešene na osnovu automatske obrade ili profilisanja, nego se primenjuje i na prikupljanje podataka u svrhu izrade profila kao i na primenu tih profila na pojedince.

Definicija

„Profilisanje" ili izrada profila se odnosi na svaki oblik automatske obrade podataka o ličnosti, koji se sastoji od upotrebe podataka o ličnosti za ocenu određenih ličnih aspekata povezanih sa pojedincem, posebno za analizu ili predviđanje aspekata

u vezi sa radnim učinkom, ekonomskim stanjem, zdravljem, ličnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca.

Iz navedene definicije proizlazi da se radi o jednoj posebnoj analizi i proceni podataka o ličnosti. Pod pojmom profilisanje moguće je ustanoviti različite modalitete primene i procene podataka o ličnosti.

Profilisanje se sastoji od tri bitna elementa:

- ✓ automatski oblik obrade,
- ✓ sprovodi se na podacima o ličnosti,
- ✓ svrha profilisanja mora da bude procena ličnih aspekata pojedinca.

Profilisanje se odnosi na „*svaki oblik automatske obrade*", a *ne „isključivo" na automatsku obradu* kao po čl. 22 OUZP. Izrada profila mora da uključi neki oblik automatske obrade, međutim obrada podataka pojedinaca nužno ne uklanja tu aktivnost.

Profilisanje je postupak koji može da bude baziran na zaključcima izvedenim iz *statističkih podataka*. Takođe sam postupak profilisanja je najčešće izveden iz *različitih izvora* kako bi se o pojedincu izveo neki zaključak ili prognoza iz već sličnih statističkih zaključaka o određenoj osobi.

Profilisanje treba da uključi automatizovanu obradu podataka o ličnosti radi *procene ličnih aspekata*, naročito radi analize *ili predviđanja u vezi sa pojedincima*. Procenjivanje se odnosi neki oblik ocenjivanja ili mišljenja o nekoj osobi. Samo klasifikovanje pojedinaca na osnovu obeležja kao što su godine, pol i visina ne dovodi nužno do izrade profila. Na to utiče *svrha klasifikacije*.[81]

PRIMER USTANOVLJAVANJE PROFILISANJA
Neko preduzeće želi da klasifikuje svoje klijente u statističke svrhe prema njihovim godinama ili polu, da bi dobilo pregled klijenata. Pritom neće biti donešena nikakva predviđanja ili izvođeni nikakvi zaključci o pojedincu. Ovde je svrha klasifikacije nije u proceni pojedinačnih obeležja, pa se zato ne radi profilisanju.

Prema nekim procenama danas društvene mreže koriste više od 52.000 ličnih atributa ili obrazaca ponašanja koji klasifikuju interesovanja ljudi. Ti podaci se koriste za analiziranje informacija ili predviđanje budućeg ponašanja ili razvoja. Što je više podataka o određenoj osobi dostupno i što duže se radi da izradi njegovog profila, to će profil osobe biti bolji i sveobuhvatniji.

Nastalo znanje i kvalitet saznanja iz profilisanja je od suštinskog značaja da bi se uopšte govorilo o svrsi profilisanja. Prema nekim mišljenjima *metode data mining* poznaju bolje neku ličnost od samih tih ličnosti i porodica.[82] Sa druge strane neki

[81] Radna grupa član 29, *Smernice o automatizovanom donošenju pojedinačnih odluka i izradi profila za potrebe Uredbe 2016/679*, 17/DE, WP251rev.01, Die Datenschutzgruppe Artikel 29, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 3. Oktober 2017, überarbeitet am 6. Februar 2018, 17/DE, str. 5, 6, 7.

smatraju da *profilisanje predstavlja samo verovatnoću*. Ono što je bitno je da znanje i saznanja koja proizlaze iz profilisanja u značajnoj meri utiču na život pojedinca. Ona se mogu dalje upotrebiti za donošenje odluka (automatsko ili neautomatsko) u vezi sa pojedincima ili grupom ljudi.[83]

PRIMER PRAĆENJE BORAVKA POJEDINCA
Radi se o praćenju posebnih osobina i ponašanja pojedinca u odnosu na to gde boravi.

PRIMER PROFILISANJE KLIJENATA UZ POMOĆ DATA WAREHOUSE
Data Warehouse se koristi u svrhu analize klijenata, tako što se u centralnoj bazi podataka analiziraju ogromne količine podataka iz različitih sistema. Pomoću rezultata analize i izveštaja donose se odgovarajuće poslovne odluke.

PRIMER PROFILISANJE UZ POMOĆ DRUŠTVENIH DODATAKA OD STRANE FEJSBUKA
Fejsbuk prati internet surfovanje odnosno saobraćaj i na taj način pravi detaljno profilisanje internet korisnika. Kada su korisnici prijavljeni (ulogovani), Fejsbuk uzima podatke sa profila korisnika, ime, e-mail adresu, listu prijatelja i stvari koje su lajkovane, ali i IP-adresu, podatke o rezoluciji ekrana, operativnom sistemu i brauzeru koji je korišćen. Vreme, datum i URL svakoga ko koristi Fejsbukov društveni dodatak „Social Plug-in". Podaci se prate, bez obzira da li je korisnik pristao i bez ikakve najave da će to biti urađeno.[84]

PRIMER SCORING
Poseban postupak procene pojedinca u kome se određene individualne osobine procenjuju uz pomoć unapred definisanih obeležja. Radi se o prognozi budućeg *mogućeg (verovatnog)* ponašanja ili stanja zasnovanog na predhodnom iskustvu, iz kojeg se izvodi *faktor rizika određene osobe*. *Kreditni scoring*: označava procenu verovatnoće i stanja, da određena osoba može vratiti kredit. Kreditni scoring se procenjuje od strane kreditnih biroa (u Srbiji je to kreditni biro Srbije, u Nemačkoj SHUFA, u Austriji KSV).[85] Iz kreditnog scoring-a može se utvrditi i bonitet odnosno *platna sposobnost određene osobe*. Tom prilikom se koriste različite kategorije ocenjivanja platne sposobnosti kao što su: istorijat

[82] Data Mining metode se odnose na softver, koji je zasnovan na automatizovanim predviđanjima predloženih rešenja na osnovu poznatih obrazaca ponašanja iz prošlosti, kao i identifikacija prethodno nepoznatih odnosa, obrazaca i trendova u vrlo velikim bazama podataka. U kontekstu Data Mining velike baze podataka se traže šabloni koji se ponavljaju. Ovo omogućava, na primer, da se putem frekvencije komunikacije ili kroz učestalost i trajanje zajedničke komunikacije u jednom delu telekomunikacione mreže, socijalni odnosi sa sigurnom verovatnoćom mogu rekonstruisati. Pored toga, moguće je otkriti sve društvene konekcije, njihovo širenje i hijerarhijske strukture koje proizlaze iz njih. Dragan Prlja, Andrej Diligenski, *Pravni aspekti neutralnosti Internet mreže*, Strani pravni život, br. 3, 2011, str. 137.

[83] European Data Protection Supervisor, *Opinion on Online Manipulation and Personal Data*, Opinion 3/2018, 19.03.2018., str. 8, 9.

[84] Andrej Diligenski, Dragan Prlja, *Fejsbuk, zaštita podataka i sudska praksa*, Institut za uporedno pravo Beograd, 2018., str. 139.

[85] Was ist Scoring?, SCHUFA, https://www.schufa.de/de/ueber-uns/ daten-scoring/ scoring/ scoring/, 31.3.2018.

plaćanja, poslovanje, struktura sredstava, struktura kapitala, pokazatelji likvidnosti, pokazatelji uspešnosti.[86] Kreditna sposobnost se nekad utvrđuje i *samo na osnovu adrese stanovanja neke oso*be, pošto je moguće sa velikom verovatnoćom utvrditi da li je određena osoba platežno sposobna.

Da li se radi o profilisanju ili o automatskom donošenju odluka (čl. 22 st. 1 OUZP) zavisiće od pojedinačnog slučaja i oklonosti slučaja.

3.4.1. Automatsko donošenje odluka, uključujući i profilisanje (čl. 22 OUZP)

Samo automatsko donošenje odluka predstavlja donošenje odluka uz pomoć tehnoloških sredstava *bez učestvovanja ljudi.*

Automatsko donošenje odluka može biti bazirano na različitim izvorima i različitim vrstama podataka:

- ✓ na podacima koje su *direktno dostavili pojedinci* (upitnik, anketa),
- ✓ na podacima koji su prikupljeni *opažanjem pojedinaca* (podaci prikupljeni pomoć „kolačića", podaci o lokaciji prikupljeni pomoću aplikacija),
- ✓ na *izvedenim podacima* (npr. koji su izvedeni iz već izrađenog profila pojedinca u postupku procene kreditne sposobnosti).

Automatsko donošenje odluka je zasnovano na *drugačijem obimu obrade podataka od profilisanja*. Stoga ono može proizlaziti iz profilisanja ili se preklapati sa profilisanjem. *Automatsko donošenje odluka dakle može postojati i bez izrade profila, a može biti i bazirano ili proizlaziti iz profilisanja.* Isto tako naravno kao što izrada profila može postojati i bez samog automatskog donošenja odluka. Osim toga moguće su situacije u praksi u kojima se u početku radi o postupku automatskog donošenja odluka, koji se kasnije može pretvoriti u postupak koji se bazira na izradi profila.

PRIMER
Kamere koje snimaju saobraćaj radi uočavanja prekršaja prekoračenja dozvoljene brzine bazirane su na postupku automatskog donošenja odluka, koji ne uključuje izradu profila. Moguće je da se automatsko donošenje odluka bazira na izradi profila, da bi se utvrdilo ponašanje pojedinaca u vožnji u određenom vremenu tj. da bi se došlo do toga da li se radi o ponovljenom prekršaju ili se radi o već sličnim prekršajima.

Samo donošenje odluke može kao što je već rečeno uključivati izradu profila, a da se ne radi pritom o automatskom donošenju takve odluke.

[86] Scoring model, scoring.rs, dobar primer scoring modela i obračunavanja sa kategorijama dat je na sajtu scoring.rs i http://www.scoring.rs/ dokumenta/Metodologija% 20Scoring% 20modela.pdf, 31.03.2018.

PRIMER
Banka pre odobravanja hipotekarnog kredita može uzeti u obzir kreditnu sposobnost zajmoprimca. Tom prilikom bankarski službenici proveravaju odluku (koja nije automatska) a koja će imati posledice po pojedince pre donošenja same odluke.

Profilisanje se može upotrebiti na različite načine:

- ✓ opštom izradom profila,
- ✓ donošenjem odluka na osnovu izrade profila,
- ✓ *isključivo automatiskim* donošenjem odluka, uključujući i profilisanje, koje proizvode pravne efekte na pojedinca ili na sličan način značajno utiču na njega (čl. 22 st. 1 OUZP).[87]

PRIMER RAZLIKA IZMEĐU tačke 2. i 3.
Kada pojedinac zatražio zajam preko interneta: ✓ odluku o odobravanju zajma donosi *bankarski službenik na osnovu profila* koji je izrađen isključivo automatskim putem (2.) ✓ odluku o odobravanju zajma donosi algoritam i ona se automatski dostavlja pojedincu, a da prethodno *nijedna osoba* nije sprovela i proverila procenu ispravnosti odluke (3.)

Ovakvim analizama ljudi OUZP određuje granice u članu 22.

Automatsko pojedinačno donošenje odluka, uključujući profilisanje

„1. Pojedinac (pogođeno lice) ima pravo da se na njega ne odnosi odluka koja se temelji *isključivo na automatskoj obradi, uključujući profilisanje*, koja proizvodi pravna dejstva koja se na njega odnose ili na sličan način značajno na njega utiču

2. *Stav 1. ne primjenjuje* se ako je odluka:

(a) *potrebna za sklapanje ili izvršenje ugovora* između pojedinca i odgovornog lica;

(b) dopuštena pravom Unije ili pravom države članice kojem podleže odgovorno lice i koje takođe propisuje odgovarajuće mere zaštite prava i sloboda kao i legitimnih interesa pojedinaca; ili

(c) temeljena na *izričitom pristanku pojedinca*.

Na ovom mestu treba primetiti 3 bitne mogućnosti zakonite obrade podataka vezanih za automatske obrade ili profilisanja koje proizlaze iz čl. 22 OUZP.

1) Naime da bi uopšte došlo do automatske obrade koja može da uključi i profilisanje neophodno je da takva obrada podataka bude *potrebna za sklapanje ili izvršenje ugovora.*

---

[87] Radna grupa član 29, *Smernice o automatizovanom donošenju pojedinačnih odluka i izradi profila za potrebe Uredbe 2016/679*, 17/DE, WP251rev.01, Die Datenschutzgruppe Artikel 29, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 3. Oktober 2017, überarbeitet am 6. Februar 2018, 17/DE, str. 8, 9.

MOGUĆA SITUACIJA U PRAKSI – PROVERA BONITETA
Banke bi mogle po ovom osnovu da obrazlože, da je za sklapanje ugovora o kreditu neophodno da se izvrši procena kreditne sposobnosti. Argumentacija banaka bi mogla ići u smeru da je to u njihovom interesu, ali i u interesu klijenata, da bi mogli da vrate kredit. Može se reći da su već ustaljene varijante scoring-a u praksi na ovaj način postale zakonite. I pored toga treba uzeti u obzir i način obrade podataka, pošto bi po OUZP *automatsko (bez učešća ljudi) odbijanje zahteva za kreditom putem interneta bilo nedopušteno* (U.t.r. 71 OUZP).[88]

MOGUĆA SITUACIJA U PRAKSI – PROFILISANJE UZ POMOĆ KOLAČIĆA
Ova zakonska osnova ne bi generalno važila za upotrebu kolačića u svrhu profilisanja, iako je naravno teoretski moguće zamisliti da je upotreba profila uz pomoć kolačića ili automatska obrada podataka nužno potrebna za sklapanje ili izvršenje ugovora. Profilisanje uz pomoć kolačića bi samim tim bilo *dopušteno samo na osnovu izričitog pristanka pojedinaca.*

2) Ako automatska obrada koja može da uključi i profilisanje nije potrebna za sklapanje ili izvršenje ugovora, onda se ova obrada podataka može zasnivati na *izričitom pristanku*. U ovom slučaju treba obratiti pažnju na punovažnost pristanka pojedinca.

MOGUĆA SITUACIJA U PRAKSI – PROFILISANJE UZ POMOĆ DATA WAREHOUSE
Kod korišćenja podataka klijenata iz Data Warehouse trebalo bi proceniti već datog pristanka klijenata, da li je u tim saglasnostima obuhvaćena nameravana obrada podataka u svrhu profilisanja. Posebno treba obratiti pažnju da li je došlo do promene svrhe obrade podataka korišćenjem Data Warehouse rešenja, odnosno da li postoji neki drugi zakonski osnov za ovakvu obradu podataka.

MOGUĆA SITUACIJA U PRAKSI – PROFILISANJE UZ POMOĆ APLIKACIJA
Kod podataka o lokaciji je moguće takođe od slučaja do slučaja argumentovati da aplikacije moraju da izvrše profilisanje korisnika, jer to proizlazi iz same prirode aplikacije (npr. aplikacije koje mere puls, gubitak kilograma, poziciju, pretrčane kilometre). Tu je moguća i argumentacija da su korisnici prihvatili opšte uslove korišćenja aplikacije. U ovom slučaju je potrebno proceniti punovažnost pristanka.

Treba imati u vidu i važno je napomenuti da je *automatsko donošenje odluka uključujući i profilisanje* (čl. 22 st. 1 OUZP) dopušteno samo u slučaju zakonskih osnova obradu baziranih na izričitom pristanku ili ugovoru sa pojedincem. *Samo profilisanje koje nije zasnovano na automatskom donošenju odluka* može biti dopušteno i po ostalim zakonskim osnovama obrade podataka (čl. 6 OUZP). Zbog toga je od izuzetnog značaja pravilno odrediti uslov dopuštenosti obrade podataka.

Identično važi i kada se radi o obradi posebnih kategorija podataka o ličnosti tzv. „osetljivih podataka". I u tom slučaju kod *samo profilisanja* treba tražiti dopuštenost obrade podataka u svim uslovima iz čl. 9 st. 2 OUZP. Profilisanje se može dobiti iz posebnih kategorija podataka ali i izvođenjem zaključaka iz podataka koji sami po

[88] Klaus M. Steinmaurer, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 86.

sebi nisu podaci iz posebne kategorije, međutim postaju osetljivi kad se kombinuju sa drugim podacima. Tako primera radi zaključci o nečijem zdravstvenom stanju mogu da se izvuku iz podataka o kupovini hrane, ako se kombinuju sa podacima o kvalitetu i energetskoj vrednosti namirnica.

Kombinovanjem podataka o zdravlju, političkim i verskim uverenjima, seksualnoj orijentaciji pojedinaca moguće je doći to prilično preciznih zaključaka.

PRIMER
U jednoj studiji podaci korisnika Fejsbuka koji su koristili funkciju „sviđa mi se" tj. lajk dugme kombinovani su sa informacijama iz ankete. Tom prilikom su istraživači tačno predvideli seksualnu orijentaciju muških korisnika u 88 % slučajeva, etničko poreklo korisnika u 95 % slučajeva, a verska uverenja korisnika (hrišćanin ili musliman) u 82 % slučajeva.

Prema mišljenju Radne grupe član 29, kada se izradom profila izvode zaključci o osetljivim sklonostima i obilježjima, rukovalac treba da obezbedi:

- ✓ da obrada bude usklađena sa prvobitnom svrhom;
- ✓ da je utvrđena zakonska osnova za obradu posebnih kategorija podataka;
- ✓ da je sprovedeno obaveštenje pojedinaca o obradi.[89]

Automatsko donošenje odluka uključujući i profilisanje (čl. 22 st. 4 OUZP) osetljivih podataka o ličnosti dopušteno je u slučaju:

- ✓ Postojanja nekog od izuzetaka iz čl. 22 st. 2 OUZP

i

- ✓ Postojanja izričitog pristanka (čl. 9 st. 2 a) OUZP) *ili* je obrada neophodna za potrebe značajnog javnog interesa, na osnovu prava Unije ili prava države članice koje je srazmerno željenom cilju i kojim se poštuje suština prava na zaštitu podataka i obezbeđuju primerene i posebne mere za zaštitu osnovnih prava i interesa lica na koje se podaci odnose (čl. 9 st. 2 g) OUZP)

i

- ✓ Postojanje odgovarajućih mera za zaštitu prava i sloboda pojedinaca

i

- ✓ Postojanje legitimnih interesa pojedinaca.

Ovako postavljena formulacija vezana za automatsku obradu uključujući i profilisanje dovodi do zaključka da je posebne kategorije podataka o ličnosti moguće obrađivati u slučaju ispunjenja sledećih uslova:

[89] Radna grupa član 29, *Smernice o automatizovanom donošenju pojedinačnih odluka i izradi profila za potrebe Uredbe 2016/679*, 17/DE, WP251rev.01, Die Datenschutzgruppe Artikel 29, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 3. Oktober 2017, überarbeitet am 6. Februar 2018, 17/DE, str. 10, 15, 16.

- ✓ Postojanje neophodnosti zaključenja/izvršenje ugovora *i* postojanja izričitog pristanka *i* postojanje odgovarajućih mera za zaštitu prava *i* sloboda pojedinaca *i* postojanje legitimnih interesa pojedinaca; ili
- ✓ Postojanje neophodnosti zaključenja/izvršenje ugovora *i* obrada je neophodna za potrebe značajnog javnog interesa *i* postojanje odgovarajućih mera za zaštitu prava *i* sloboda pojedinaca *i* postojanje legitimnih interesa pojedinaca; ili
- ✓ Postojanje obrade koje je neophodna za potrebe značajnog javnog interesa *i* postojanje odgovarajućih mera za zaštitu prava i sloboda pojedinaca *i* postojanje legitimnih interesa pojedinaca; ili
- ✓ Postojanje izričitog pristanka *i* postojanje odgovarajućih mera za zaštitu prava i sloboda pojedinaca *i* postojanje legitimnih interesa pojedinaca.

3) I pored prve dve mogućnosti za zakonitu obradu ovih podataka, predviđena je *otvorena klauzula* (čl. 22 st. 2 b) OUZP), koja omogućava državama članicama da samostalno u potpunosti reguliše ovu materiju. Stoga se može reći da *iako postoji odredba iz člana 22* st. 1 OUZP, *ova materija može potpuno drugačije biti regulisana u nekoj od država članica EU*. To predstavlja veliku šansu da se ova materija detaljnije i bolje uredi, kao i da se izbegne pravna nesigurnost stvorena članom 22 OUZP.

OUZP u čl. 22 st. 3 određuje da je *neophodno preduzeti adekvatne zaštitne mere* pri automatskoj obradi podataka ili profilisanju. Takođe *osetljivi podaci o ličnosti* (iz čl. 9 st. 1 OUZP) se mogu obrađivati u svrhe automatske obrade podataka ili profilisanja, samo *ako postoji izričita saglasnost pojedinca* ili ako je takva *obrada nužna za potrebe javnog interesa* države članice EU.

Od izuzetnog značaja je da *bi se uopšte moglo govoriti o zakonitoj obradi podataka iz čl. 22 OUZP*, *neophodno je predhodno izvršiti procenu rizika posledica po pojedinca* (čl. 35 st. 3 a) OUZP). Stoga je neophodno pre procene zakonitosti obrade podataka na osnovu čl. 22 OUZP najpre proceniti rizik po prava pojedinca, pa bi se pravno moglo reći da je čl. 35 st. 3 a) OUZP jedna vrsta *predhodnog pitanja (predhodne procene), bez čijeg odgovra nije moguće ustanoviti zakonitu obradu podataka.*

NAPOMENA | *Bez procene rizika po pojedince nema zakonite obrade podataka u svrhu automatske obrade podataka ili profilisanja.*

Zbog rizika po prava pojedinaca u vezi sa automatskim donošenjem odluka uključujući i profilisanjem, rukovaoci treba naročitu pažnju da posvete *transparentnosti*. To se posebno odnosi na jednostavne, lako dostupne *informacije o automatskoj obradi*. Rukovalac je dužan da *pre nameravane obrade podatka* ukoliko obrađuje podatke na osnovu čl. 22 st. 1 OUZP dostavi informacije o:

- ✓ sprovođenju aktivnosti automatskog donošenja odluka uključujući i o profilisanju,

- ✓ logici obrade,
- ✓ značaju i predviđenim posledicama takve obrade.

Pružanje tih informacija omogućava *ispunjavanje zahteva o zaštitnim merama* (čl. 22 st. 3 OUZP) kao što su *pravo na intervenciju od strane rukovaoca, pravo izražavanja svog stava, prava na osporavanje odluke*.

U cilju ostvarivanja načela transparentnosti rukovalac je takođe u obavezi da pojedinca informiše o *logici obrade ili o kriterijumima* na osnovu koji se bazira donošenje odluka. Ova objašnjenja ne treba prema mišljenju Radne grupe član 29 da se odnose na složene i komplikovane opise algoritama ili da nužno u potupnosti otkriju koji se algoritam koristi. Potrebno je da se dostave informacije vezane za automatsko donošenje odluke, koje bi bile sveobuhvatne i koje bi pojedinci razumeli.

Ove informacije treba da dostavi ne samo shodno čl. 13 st. 2 f) i čl. 14 st. 2 g) OUZP (pružanje informacija nezavisno od toga da li su prikupljene direktno od pojedinca ili iz drugih izvora) *nego i shodno 15 st. 1 h) OUZP kod prava na pristup informacijama*.

PRIMER Ocena kreditne sposobnosti za dobijanje zajma
Nezavisno od toga da li su informacije o oceni kreditne sposobnosti dobijene od kreditnog instituta ili je informacije prikupio i obradio sam rukovalac, on je u obavezi da pruži informacije o logici obrade ili o kriterijumima na osnovu kojih bazira svoju odluku. To mogu biti sledeće informacije: ✓ informacije koje pojedinac navodi u obrascu zahteva, ✓ informacije o prethodnom ponašanju s obzirom na račun, uključujući neplaćene obaveze, ✓ informacije iz službenih javnih evidencija kao što su informacije iz evidencija o prevarama i evidencija o nesolventnosti. Rukovalac treba da pruži informacije o tome da se metode koje se koriste za ocenjivanje kreditne sposobnosti redovno testiraju, da bi se obezbedilo da ostanu poštene, efektivne i nepristrane.

Rukovalac treba da pruži i kontakt podatke za intervencije pojedinaca u pogledu ponovnih razmatranja odluka o odbijanju (čl. 22 st. 3 OUZP).

Rukovalac je u obavezi da pruži *informacije o značaju i predviđenim posledicama takve obrade*. Radi jednostavnosti i razumljivosti preporučuje se navođenje konkretnih primera mogućih posledica (npr. kod premije osiguranja vezanog za motorna vozila i praćenje ponašanja vozača, treba objasniti da prebrzo kočenje, naglo ubrzavanje, uopšte opasne navike utiču na visinu premije osiguranja).

U kontekstu izrade profila i donošenja automatskih odluka *prava pojedinaca* su osnažena naročito u pogledu obaveštavanja pojedinaca o ovoj vrsti obrade. Uzimajući u obzir načelo transparentnosti (U.t.r. 60 OUZP), potrebno je da rukovaoci na jasan i razumljiv način objasne cilj profilisanja ili donošenja automatskih odluka.

Ako se podaci obrađuju na osnovu automatskog donošenja odluka uključujući i profilisanje tada je neophodno da se objasni tačna svrha obrade: izrada profila *i* donošenje automatskih odluka na osnovu izrađenih profila.

Transparentnost prema pojedincima treba da uključi i obaveštenja o tome kome će se podaci prenositi. Osim toga rukovaoci treba posebno da napomenu *pravo prigovora pojedinaca,* ako se podaci obrađuju na osnovu automatskog donošenja odluka uključujući i profilisanje (čl. 22 st. 1 OUZP). Pravo na prigovor u pogledu izrade profila postoji *nezavisno od toga da li se sprovodi isključivo automatsko donošenje odluka ili ne.*

Pojedinci imaju pravo da dobiju informacije (*pravo na pristup informacijama*) o pojedinostima vezanim za njihove podatke koji se koriste za izradu profila, uključujući kategorije podataka koje se koriste za izradu profila (čl. 15 OUZP).

Rukovalac treba pored informacija koji su navedeni posebno da dostavi informacije o podacima koji se unose i koriste u izradi profila (čl. 15 st. 1 OUZP). Osim toga pristup informacijama o profilu uključuje i detaljne informacije o segmentima u koje je pojedinac kategorisan.

Ove obaveze rukovaoca se u mnogome razlikuju od prava prenosivosti. Shodno ovom pravu (čl. 20 OUZP) rukovalac je u obavezi da dostavi samo one podatke koje mu je pojedinac sam pružio ili koje se rukovalac sam zabeležio, a ne i podatke o tome kako je dobijen profil.

Zaštita rukovaocima omogućena je u slučajevima profilisanja, ako se prilikom ostvarivanja ovog prava otkriju poslovne tajne ili dođe do povrede prava intelektualne svojine (U.t.r. 63 OUZP). Rukovaoci ne mogu da se pozovu na zaštitu svojih poslovnih tajni kao izgovor za uskraćivanje pristupa ili odbijanje pružanja informacija pojedincu. Rukovaoci takođe ako je to moguće treba da omoguće daljinski pristup zaštićenom sistemu koji bi pojedincu omogućio direktan pristup njegovim podacima o ličnosti (U.t.r. 63 OUZP).

Profilisanje može dovesti do netačnih prognoza, predviđanja, pogotovu ukoliko su podaci netačni ili pogrešno interpretirani ili pogrešno izvedeni iz konteksta. Takođe u praksi pri automatskoj izradi profila moguće je da je algoritam pogrešno programiran ili koristi za predviđanje pogrešnu korelaciju. Ovo svakako može biti od značaja za pojedince u pogledu primene *prava na ispravku podataka*. Ukoliko pojedinci saznaju za kategorizaciju ili prognozu koja je pogrešna, imaju mogućnost da zatraže ispravku podataka. Pravo na ispravljanje podataka uključuje i mogućnost pojedinca da svoje podatke dopuni.

Pravo na brisanje i na ispravku podataka se primenjuje kako na *ulazne podatke o ličnosti* (podatke koji su korišćeni za izradu profila) i na *izlazne podatke* (sam profil, prognoza, predviđanje vezano za određenu osobu).

Rukovalac je u obavezi da izričito skrene pažnju pojedincu o *pravu na prigovor* (čl. 21 st. 1 i 2 OUZP) i to mora da učini jasno i odvojeno od ostalih informacija (čl. 21 st. 4 OUZP).

Pravo prigovora je posebno predviđeno i u slučajevima obrade zasnovane na „javnom interesu“ (čl. 6 st. 1 e) OUZP) ili „legitimnim interesima“ (čl. 6 st. 1 f) OUZP). Ukoliko pojedinac uloži prigovor na obradu (uključujući i na izradu profila), rukovalac mora da prekine (ili ne započine) postupak izrade profila. *Izuzetak* od ovoga je u slučaju da rukovalac može da dokaže *postojanje legitimnih intersa za obradu koji prevazilaze interese, prava i slobode pojedinaca*.

Stoga se preporučuje da rukovalac sprovede *test ravnoteže interesa* i za argumentaciju u cilju ostvarivanja prava prigovora pojedinaca. Ovaj test može poslužiti kao valjan dokaz u smislu ostvarivanja načela društvene odgovornosti.

Preporučuje se procena vezana za:

- ✓ važnost izrade profila u odnosu na konkretan cilj,
- ✓ uticaj izrade profila na interese, prava i slobode pojedinaca (koji treba da budu ograničeni na najmanju moguću meru koja je potrebna za ostvarivanje konkretnog cilja),
- ✓ test ravnoteže interesa.

Test ravnoteže interesa (čl. 21 st. 1 OUZP) se ovde razlikuje bitno u odnosu na čl. 6 st. 1 f) OUZP, zato što se zahteva da legitimni (pretežniji) interesi rukovaoca budu *uverljivi*. Samim tim treba da postoji jasan i nedvosmislen interes da bi rukovaoci odbili pravo prigovora po ovom osnovu.

U slučaju *direktnog marketinga* (uključujući i profilisanje) pravo prigovora (čl. 21 st. 2 OUZP) može se koristiti bezuslovno. To podrazumeva da nije neophodno obaviti test ravnoteže interesa. Ovo pravo se može ostvariti u bilo koje vreme i besplatno (U.t.r. 70 OUZP).

Sam prigovor u slučaju automatske obrade uključujući profilisanje (i posebno ako se profilisanje koristi u marketinške svrhe) ima *dejstvo koje obavezuje rukovaoca na brisanje podataka* (čl. 17 st. 1 c) OUZP). *Izuzetak* od ovoga je u slučaju da ne postoje preovlađujući zakonski razlozi za obradu. U slučaju upotrebe profila u marketinške svrhe (direktan marketing), podaci moraju da budu obrisani![90]

Ako se kao osnova za obradu podatka u postupku automatskog odlučivanja koje uključuje i profilisanje (kada se radi o obradi podataka koji ne spadaju u posebne kategorije) uzima *zaključenje/izvršenje ugovora* (čl. 22 st. 2 a) OUZP) *ili izričit pristanak* (čl. 22 st. 2 (c) OUZP), zahteva se (čl. 22 st. 3) da rukovalac sprovede *odgovarajuće mere zaštite prava i sloboda i legitimnih interesa pojedinaca*.

Takođe čl. 22 st. 2 b) OUZP *pravo Unije ili pravo države članice* kojim se dopušta obrada mora da uključi i odgovarajuće zaštitne mere.

U te mere spadaju mogućnosti za pojedince u pogledu intervencije, izražavanja ličnog stava i osporavanja odluke.

Prilikom korišćenja automatskog donošenja odluka uključujući i profilisanje *neophodno je stoga omogućiti intervenciju*. Na taj način bi bilo omogućeno pojedincima s obzirom na značajno zadiranje u njihova prava, da se odluka uz dodatne informacije koje oni dostave i ostale podatke koje ima rukovalac adekvatno i tačno donese.[91]

Podaci o deci i automatska obrada podataka uključujući i profilisanje predstavljaju pitanje koje OUZP ne razmatra posebno. Naime, sam čl. 22 OUZP

[90] *Ibidem*, str. 16, 17, 18, 19.

[91] *Ibidem*, str. 27, 28.

ne pravi razliku u odnosu na to da li se u postupku automatske obrade podataka uključujući i profilisanje radi o podacima koji se odnose na decu ili ne.

U.t.r. 71 OUZP navodi da se *isključivo automatsko donošenje odluka uključujući i profilisanje ne sme odnositi na decu*. Stoga ova uvodna tačka razmatranja *nema obavezujuće dejstvo*, ali bi se moglo reći da daje smer i tumačenje namere zakonodavca. I pored toga ne može se reći da je ovakva obrada podataka dece zabranjena. Ukoliko bismo uzeli kao primer onlajn okruženje, čak i da postoji ovakva zabrana, ona bi bila u praksi neprimenljiva (uzimajući u vidu npr. ciljano oglašavanje po osnovu kolačića). U.t.r. 38 OUZP naglašava zaštitu podataka dece zbog njihovog posebnog položaja (rizika, svesnosti, posledica) prilikom obrada u svrhe marketinga ili stvaranja ličnih ili korisničkih profila (misli se pre svega na onlajn pružanje usluga).

Može se zaključiti da rukovaoci ukoliko žele da primene tehnike automatskog donošenja odluka uključujući i profilisanja, treba da se pridržavaju zahteva iz čl. 22 OUZP.

OUZP podstiče izradu kodeksa ponašanja u kojima treba regulisati „informisanje i zaštitu dece i način pribavljanja roditeljskog prava nad decom" (čl. 40 st. 2 g) OUZP).[92]

Procena uticaja u vezi sa zaštitom podataka predstavlja bitnu metodu, kojom se upravlja sa rizicima. Procenom rizika i posledica po pojedince preduzimaju se adekvatne mere da se spreči nastupanje rizika po pojedince i da se dokaže usklađenost sa OUZP. Tako primena ove metode dovodi do toga da se za automatske obrade uključujući profilisanje, preduzmu pre svega adekvatne mere zaštite pojedinca za obrade koje same po sebi nose visok rizik.

Zbog toga je i predviđena obaveza sprovođenja procene uticaja u vezi sa zaštitom podataka (čl. 35 st. 3 a) OUZP): „sistematske i obimne procene ličnih aspekata u vezi sa fizičkim licima koja se zasniva na automatizovanoj obradi, uključujući i izradu profila, i koja je osnov za donošenje odluka koje proizvode pravno dejstvo u odnosu na fizičko lice ili na sličan način značajno utiču na fizičko lice".

Analizom ove norme može se uočiti da se za primenu ove norme ne zahteva da automatska obrada bude „isključiva", već je dovoljno da se obrada podataka „*zasniva na automatskoj obradi*". Na taj način treba primeniti ovu normu i u slučaju kada se ne radi o isključivoj automatskoj obradi i u slučajevima kada se radi o isključivoj automatskoj obradi (čl. 22 st. 1 OUZP). Radi se zapravo o situacijama kojima se započinje obrada podataka, pa je stoga intencija zakonodavca bila da se u modelu obrade podataka dozvoli pre svega intervencija ljudi, a ne mašina, kako bi se smanjio rizik po pojedince.

Mere kojima bi moglo da dođe do umanjenja rizika su:

- ✓ informisanje pojedinaca o postojanju postupka automatskog donošenja odluka i o njegovoj logici;
- ✓ objašnjavanje važnosti i predviđenih posledica obrade za pojedince;

[92] *Ibidem*, str. 29, 30.

- ✓ omogućavanje pojedincu načina da ospori odluku i
- ✓ omogućivanje pojedincu da izrazi svoj stav.

Treba imati u vidu da je *imenovanje ovlašćenog lica za zaštitu podataka obavezno* ako se osnovne delatnosti rukovaoca ili obrađivača sastoje iz radnji obrade koje zbog svoje prirode, obima i/ili svrha zahtevaju redovno i sistematsko masovno praćenje lica na koja se podaci odnose. Radi se pre svega o profilisanju ili automatskom donošenju odluka, koje predstavljaju osnovnu delatnost rukovaoca ili obrađivača (čl. 37 st. 1 b) OUZP).[93]

3.4.2. BIG DATA

U svetu informacionog društva danas je ovaj pojam postao neizbežan. Može se reći da je *profilisanje jedno od bitnih obeležja pojma Big Data*, pa je stoga potrebno razumeti i razliku profilisanja u odnosu na Big Data.

Pojam i definicija *Big Data nisu regulisani u OUZP*, ali će zbog izuzetnog značaja za razvoj modernih tehnologija i mogućnosti biti razmatran.

Značenje ovog pojma se pre svega odnosi na *što je moguće veću količinu podataka i što je moguće precizniju prognozu (profilisanje)* kao *i na komercijalno iskorištavanje ovakve prognoze.*[94]

Pojam Big Data je definisan od strane EU parlamenta u njegovoj rezoluciji od 20.02.2017.godine: "označava prikupljanje, analizu i učestalo akumuliranje velikih količina podataka, uključujući i podatke o ličnosti, iz različitih izvora, koji se automatski obrađuju uz pomoć kompjuterskih algoritama i naprednih tehnika obrade podataka za koje se koriste i snimljeni podaci i podaci preneseni strujanjem (streaming) kako bi se dobile određene korelacije, trendovi i uzorci (analiza velikih podataka)".[95]

Ukoliko se ovaj pojam želi definisati potrebno je uočiti *6 bitnih obeležja*:

- ✓ Pojam Big Data najčešće, ali *ne mora uvek sadržati podatke o ličnosti*. Stoga je u pojedinačnom slučaju potrebno proceniti važenje OUZP.
- ✓ Pojam „Big" se pre može shvatiti u *kvantitativnom*, nego u kvalitativnom smislu. Sam kvalitet podataka nije dakle presudan za definisanje ovog pojma, već količina podataka.[96]
- ✓ Suštinski element pojma Big Data je *uspostavljanje korelacije.* Radi se najčešće o *podacima koji nisu strukturisani* i koji se *povezuju uz pomoć*

[93] *Ibidem*, str. 31, 32.

[94] Klaus M. Steinmaurer, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 88.

[95] Entschließung des EU-Parlaments über die Folgen von Massendaten für die Grundrechte: Privatsphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)), 20.2.2017. slovo A.

[96] *Ibidem*. slovo B.

algoritma da bi se *dobili odgovori na određena pitanja uz prikazivanje verovatnoće*.

- ✓ Da li će se određeni izvor podataka iskoristiti, potrebno je ispitati pojedinačno, nezavisno od toga kakav će biti rezultat.

1. Što je veća količina podataka i što je veći kvalitet podataka*, utoliko je rezultat odgovora na određeno pitanje tačniji.*
2. Sadržina informacija *koja se pokaže iz nekog rezultata, nije proizvod samo jednog podatka već* veze sa ostalim podacima.[97]

Big Data je danas veliki biznis. U svetu postoje velike firme koje se bave analizom velike količine podataka kao što su Acxiom, Datalogix, Rapleaf, Core Logic, PeekYou. Acxiom je jedna od najvećih kompanija u ovoj oblasti, čiji je promet u 2017. godini bio veći od milijardu dolara, a kompanija je upravljala sa 15.000 baza podataka i imala preko 7000 klijenata i preko 700 miliona aktivnih profila korisnika.[98]

PRIMER UBER
Travis Kalanick generalni direktor kompanije Uber, jer zaradio i izgradio imperiju od njegove firme uz pomoć Big Data. Model poslovanja se sastoji u prikupljanju, korišćenju podataka preko mobilne aplikacije, koja omogućava korisnicima da pronađu vozača koji se spreman da ih odveze do željene destinacije. Uber kontroliše i snima podatke o svakoj vožnji njegovih korisnika i koristi ih kako bi podesio tarife, angazovao potrebne resurse i odredio potražnju. Pored toga se vrši detaljna analiza javnog prevoza u gradovima, gde je ovaj servis dostupan. Na taj način je Uber u stanju da pruži svoje usluge u delovima grada gde javni prevoz nije dostupan.[99]

PRIMER REKLAMIRANJE
Upotreba velikih količina podataka „big data“ za razliku od profilisanja ne vodi do toga da neka firma tačno zna gde se određena osoba nalazi, koja interesovanja ima da bi reklama bila poslata. Na ovom primeru može se govoriti o dopuštenom ili nedopuštenom marketingu, u zavisnosti od toga da li je obrada podataka zakonita. Za razliku od profilisanja kod upotrebe big data je moguće uz samu analizu pretraživanja po internetu, *bez saznanja o korisnicima* npr. adrese ili broja telefona*, doći do rezultata da se radi o muškarcu od 20-30 godina, koji nije oženjen, ali je dobrog imovinskog stanja.* Do ovog rezultata je moguće doći tako što internet korisnik pretražuje i posećuje sajtove za upoznavanje redovno, a koristi kao kriterijume neudate žene od 20-30 godina. Osim toga ova osoba bar jedanput nedeljno pretražuje luksuzne restorane, pa je stoga zaključak da je ona boljeg imovinskog stanja. Da li su ovi zaključci tačni ili nisu, nije od značaja za samu firmu koja se reklamira, da bi korisnik interneta dobio ciljanu reklamu. Savetuje se da firme koje se reklamiraju na ovaj način, dobro procene tehničke mogućnosti (čl. 35 OUZP) i saglasnosti obrade podataka sa OUZP.

[97] Klaus M. Steinmaurer, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 82.

[98] Markus Morgenroth, *Datenhandel und Big Data,* c't Magazin für Computer und Tehnik, 1/2017, str. 64.

[99] Bernard Marr, *Kako zaraditi milijardu dolara od Big Data-e*, IT Exclusive News, 5.7.2015.

PRIMER INDUSTRIJA 4.0
U okviru industrije 4.0 Big Data se primenjuje pre svega u autoindustriji kod *autonomnih i delimično autonomnih vozila*. Da bi roboti koji učestvuju u sklapanju vozila mogli međusobno da komuniciraju potrebni su Big Data programi za analizu i nova prenosna tehnologija komunikacije. Uređaj koji služi za prenosnu tehnologiju komunikacije je Eternet, koji omogućava prenos podataka od tačke A do tačke B velikom brzinom. Na tlu Evrope u ovoj oblasti prednjače Simens, Audi, Boš, BMW.[100] U SAD smo 2016. godine imali slučaj sudara potpuno autonomnog vozila marke Tesla S koji se sudario sa jednim kamionom. Još jedan slučaj se dogodio iste godine u Pensilvaniji, gde je automobil Tesla X udario o zaštitnu ogradu i prevrnuo se. Ovi slučajevi nameću i etička pitanja, koja neminovno treba rešiti.[101] [102]

PRIMER INTERNET OF THINGS
Pojam internet stvari (Internet of Things) označava međusobno *povezivanje putem interneta* predmeta, automobila, gradova, životinja, ljudi. U svakodnevnom govoru je poznatiji kao pametni gradovi, televizori, naočare itd. *Pametni predmeti* poput *umreženih mobilnih uređaja* (pametnih telefona) sa aplikacijama za vežbanje prikupljaju ogromne količine podataka o ličnosti (čak osetljivih podataka o ličnosti). Ovi podaci se onda razmenjuju i koriste u različite svrhe, a glavni kupci ovih podataka su osiguravajuća društva, koja za ove podatke daju umanjenje cene ako im se podaci putem pametnih uređaja prosleđuju. U svemu ovome analiza podataka uz pomoć Big Data se javlja kao nužna potreba. Napredne streaming analitičke tehnologije kao SAS Event Stream Processing nisu određene da nadziru samo određene uslove ili vrednosti, već mogu da predvide i budući razvoj i istraže kompleksne probleme.[103]

Iz navedenog može se zaključiti da je glavni problem Big Data danas vezan za nestrukturisane podatke koji se međusobno povezuju. Upravo možda i suštinska razlika u odnosu na profilisanje je ta što se kod Big Data *podaci sklapaju iz potpuno različitih izvora* i na osnovu toga se dobija procena. Sa stanovišta zaštite podataka je *teško odrediti vezanost za svrhu upotrebe* određene aplikacije kao *i sam pristanak* kada se radi o tolikoj količini podataka iz različitih izvora. Iz toga proizlazi da *je teško ispuniti osnovne principe zaštite podataka*.

Pošto je profilisanje jedan od bitnih elemenata Big Data, mogao bi se primeniti isti princip. Stoga da *bi se uopšte moglo govoriti o zakonitoj obradi podataka, neophodno je predhodno izvršiti procenu rizika posledica po pojedinca i proceniti svaku Big Data aplikaciju* (čl. 35 st. 3 a) OUZP). I u slučaju Big Data pravno bi se

[100] Martin Stepanek, Industrie 4.0 benötigt ein neues Ethernet, https://futurezone. at/ science/industrie-4-0-benoetigt-ein-neues-ethernet/ 96.443. 773, 01.04.2018.

[101] Sascha Mattke, *Autonome Autos: Entscheidungen von Systemen für autonomes Fahren sind kaum nachvollziehbar,* https://www.heise.de/newsticker/meldung/Autonome-Autos-Entscheidungen-von-Systemen-fuer-autonomes-Fahren-sind-kaum-nachvollziehbar-3264695.html, 04.04.2018.

[102] U Nemačkoj je polovinom maja 2017. godine donešen zakon, kojime je ova materija regulisana. Pored odgovornosti predviđeni su i propisi vezani za zaštitu podataka. Videti Straßenverkehrsgesetz (StVG), https://www.gesetze-im-internet.de/stvg/, 05.04.2018.

[103] Thomas H. Davenport, The Analytics of Things, *Analytics als Schlüssel zum Internet der Dinge*, https://www.sas.com/de_ch/insights/big-data/internet-of-things.html, 05.04.2018.

moglo reći da je čl. 35 st. 3 a) OUZP jedna vrsta *predhodnog pitanja (predhodne procene)*, bez čijeg odgovora nije moguće ustanoviti zakonitu obradu podataka.

NAPOMENA	*Bez procene rizika po pojedince nema zakonite obrade podataka u svrhu Big Data.*

Na taj način su proizvođači autonomnih vozila, proizvođači smart uređaja, operatori društvenih mreža, operatori aplikacija Big Data dužni su da pre otpočinjanja obrade podataka implementiraju rešenja zasnovana na principu *Privacy by design i Privacy by default*. Upravo za ovaj pristup se zalagao i EU parlament u njegovoj rezoluciji od 20.02.2017.g., uključujući metode anonimizacije, pseudonimizacije i kriptografije podataka.[104]

U svetlu koncepta „prava na zaborav" u vezi sa Big Data bi se moglo uvesti novo pravilo „*veliko brisanje*". Upravo u na tom polju postoji veliki izazov za kompanije i veliki rizik, kad, koje podatke i u kom roku obrisati. Stoga se savetuje da se poslovni modeli zasnovani na Big Data dobro osmisle i prilagode OUZP, pošto rizici mogu biti veći od dobiti.[105]

3.5. Odgovorna lica za zaštitu podataka

Prava i obaveze u pri obradi podataka skica

Prava	*Obaveze*	*Obaveze po nalogu*
Pojedinac/pogođeno lice (čl. 4 br. 1 OUZP)	Rukovalac (čl. 4 br. 7 OUZP)	Obrađivač (čl. 4 br. 8 OUZP), ukoliko postoji
	Zajednički rukovaoci (čl. 26 OUZP), ukoliko postoje	

3.5.1. Rukovalac (čl. 4 br. 7 OUZP)

Pre nego što definišemo pojam rukovaoca, najpre bi trebalo uočiti problematiku engleskog prevoda pojma „controller". U srpskom zakonodavstvu i praksi je uobičajen termin „rukovalac", koji se ne može reći da je adekvatan i da obuhvata sve aktivnosti i odgovornosti ovog osnovnog subjekta u čitavom lancu obrade podataka. Čini se da bi *najadekvatniji termin* bio „odgovorno lice za obradu podataka ili samo *odgovorno lice*", kako je definisan na nemačkom jeziku.[106] Zbog ustaljenog upotrebljavanja u srpskoj praksi u daljem tekstu biće u upotrebi reč „rukovalac".

[104] Entschließung des EU-Parlaments über die Folgen von Massendaten für die Grundrechte: Privatsphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)), 20.02.2017, tč. 16 i 17.

[105] Oliver Schonschek / Nico Litzel, Big Data erfordert auch das große Löschen, Big Data und Datenschutz, Teil 3, https://www.bigdata-insider.de/big-data-erfordert-auch-das-grosse-loeschen-a-539571/, 01.04.2018.

[106] Hrvatski termin je voditelj obrade, takođe u duhu našeg jezika bi se mogli koristiti i termini nalogodavac (posebno kod ugovora sa obrađivačima ili nalogoprimcima), glavni obrađivač, upravljač podacima. Svi ovi termini nisu dovoljno precizni i imaju svoje nedostatke, jer ne obuhvataju sve odgovornosti rukovaoca.

Definicija

„*Rukovalac***“** je fizičko ili pravno lice, telo javne vlasti, agencija ili drugo telo, koje samo ili zajedno sa drugima odlučuje o svrhama i sredstvima obrade podataka o ličnosti; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, tada rukovalac ili rukovaoci mogu biti predviđeni posebni kriterijumi za njegovo imenovanje na osnovu prava Unije ili prava države članice.

Sama definicija je u potpunosti preuzeta iz Direktive o zaštiti podataka 95/46/EC. Ona je višeslojna i sadrži više elemenata, koji prema mišljenju Radne grupe član 29 obuhvataju:

- ✓ „fizičko ili pravno lice, telo javne vlasti, agencija ili drugo telo“;
- ✓ „samo ili zajedno sa drugima“;
- ✓ „odlučuje o svrhama i sredstvima obrade podataka o ličnosti“.[107]

Prvi element „fizičko ili pravno lice, telo javne vlasti, agencija ili drugo telo“ se odnosi na to *ko može biti odgovoran* i *za koga iz odgovornosti nastaju obaveze*. Spektar odgovornih lica se kreće od pravnih lica, fizičkih lica, tela javnih vlasti, pa sve to nekih drugih tela.

Generalno se može reći, da ukoliko nije nedvosmisleno jasno da je fizičko lice odgovorno, da li se radi o odgovornom licu u vidu *preduzeća ili telu javne vlasti* (institucije). Često se dešavalo u praksi da se imenuje ovlašćeno *lice koje je odgovorno za obradu podataka*. Isto važi i za odgovorno lice za zaštitu podataka (eng. Data Protection Officer). Takva imenovana lica *ne predstavljaju rukovaoce* u smislu OUZP.

Sa druge strane odgovornost *fizičkog lica* se ustanovljava, ako ono radi u nekoj firmi ili telu javne vlasti, a *iskoristi podatke u sopstvene svrhe i izvan firme ili tela javne vlasti*. Tada ova osoba predstavlja *rukovaoca i odgovorna* je u smislu OUZP.

Ovaj element je od presudnog *značaja za utvrđivanje odgovornosti i kažnjavanje.* Pored toga je bitan, kada u procesu obrade podataka učestvuje više odgovornih lica, *radi ostvarivanja prava pojedinaca* (čl. 15-22 OUZP) kao i za sam *nadzor od strane nadzornih organa za zaštitu podataka*. U krajnjoj liniji je ovaj element *od suštinskog značaja i za primenu same OUZP*.[108]

Treba imati u vidu da je za utvrđivanje rukovaoca i shodno definiciji OUZP (videti drugi deo definicije) predviđena *„otvorena klauzula“ i mogućnost* da države članice EU drugačije regulišu rukovaoce posebnim zakonima.

---

[107] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje 1/2010 o pojmu rukovaoca i obrađivača*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, 00264/10/DE, WP 169, str 10.

[108] *Ibidem*, str. 19, 20, 21.

Uloga rukovaoca može nastati na više načina:

- ✓ *Eksplicitno kao pravni osnov*: Otvorenom klauzulom omogućena je odrediti rukovaoca za neku obradu podataka putem prava EU ili prava država članica. Tada treba definisati pored rukovaoca, svrhu ili svrhe obrade podataka, kategorije podataka i primaoce podataka.
- ✓ *Implicitna odgovornost*: Kada odgovornost nije regulisana zakonom, ona se može izvesti iz opštih odredbi ili uobičajene prakse (npr. poslodavac je rukovalac u odnosu na podatke svojih zaposlenih).
- ✓ *Odlučivanje o svrhama i sredstvima:* Kada se rukovalac određuje na osnovu odlučivanja. Radi se o faktičkom i činjeničnom odlučivanju o svrhama i sredstvima.[109]

Drugi element „samo ili zajedno sa drugima" se odnosi na mogućnost da ne bude samo jedan odgovoran rukovalac i da može postojati i *više odgovornih rukovalaca za jednu obradu podataka.* To je slučaj posebno kada se odgovornost odnosi na *jednu te istu obradu podataka, u kojoj podjednako odlučuju više rukovalaca i samim tim imaju podjednaku odgovornost*.

Za utvrđivanje da li se radi o samo jednom odogovornom rukovaocu ili o više njih, potrebno je najpre postaviti pitanje: Da li o svrhama i sredstvima obrade podataka o ličnosti odličuje jedna ili više osoba (preduzeća, tela javnih vlasti)?

Potrebno je ustanoviti *mogućnost zajedničke kontrole*. Od pomoći mogu biti i međusobni ugovori, pogodbe itd.

O zajedničkoj kontroli može se govoriti, *kada jedna strana odlučuje o svrisi a druga strana pruža neophodna sredstva* obrade podatka o ličnosti. Na taj način je bitno napraviti razliku u tome da rukovaoci koji sarađuju ne predstavljaju uvek zajednička odgovorna lica (rukovaoce). Bitno je da *sama razmena podataka bez zajedničke svrhe ili sredstva*, predstavlja *prenos podataka o ličnosti*.

Pošto je *zajednička obrada podataka od strane više rukovaoca* (odnosno zajednički rukovaoci) regulisana u čl. 26 OUZP, tome će biti posvećena posebna pažnja u narednom poglavlju.

Treći element „odlučuje o svrhama i sredstvima obrade podataka o ličnosti" je po mišljenju Radne grupe član 29 *suštinski element definicije rukovaoca*. Pitanje *ovlašćenja odlučivanja ili nadležnosti*, kada nije regulisano propisima EU ili država članica je suštinski element utvrđivanja rukovaoca. Sposobnost odlučivanja o obradi podataka je dakle od značaja za procenu ovog elementa. Tako se mogu najpre postaviti sledeća pitanja: Ko odlučuje o obradi podatka? Ko je prouzrokovao obradu podataka? Koji je razlog za obradu podataka „pitanje zašto"?

Moguća je i u praksi česta situacija gde se uloga rukovaoca prenosi na neko mesto, koje nije u stanju da donosi odluke (npr. kod outsourcing ugovora, ponuđača cloud usluga itd.), ali koje odlučuje o sredstvima obrade podataka. Upravo se *na ponuđače servisa* poput cloud-a *prenose sredstva obrade podataka poput tehničkih*

[109] Bernhard Horn, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 155, 156.

i organizacionih mera. Sredstva se o u ovom kontekstu ne odnose samo na tehničke i organizacione mere, već i na sveobuhvatno pitanje – *kako se podaci obrađuju?* Tu se pre svega misli na pitanja vezana za zakonitost obrade podataka (koji podaci se obrađuju, kome se prosleđuju, kada se brišu). [110]

Stoga bi odlučujuće pitanje bilo: Da li više od jedne strane odlučuje o svrhama *i suštinskim elementima sredstava* obrade podataka?[111]

PRIMER RUKOVALAC – ADVOKATI
Advokat koji zastupa pred sudom svoje klijente obrađuje pritom podatke o ličnosti. Kao pravni osnov obrade podataka je punomoćje klijenta, iako kod punomoćja naglasak nije na obradi podataka nego na zastupanju pred sudom. Generalno se može reći da zanimanja preduzetnika ispunjavaju pojam rukovaoca, pošto istupaju kao samostalno odgovorna lica.[112]

PRIMER RUKOVALAC – DRUŠTVENE MREŽE, KORISNICI
Društvene mreže daju prostor njihovim korisnicima da objavljuju i razmenjuju informacije. *Društvene mreže* su rukovaoci, pošto odlučuju o sredstvima i ciljevima obrade podataka. *Korisnici društvenih mreža* postavljaju, objavljuju podatke, fotografije trećih lica i oni se mogu klasifikovati kao rukovaoci, *ukoliko njihove aktivnosti ne odnose isključivo na lične ili porodične aktivnosti* (čl. 2 st. 2 b) OUZP).[113]

PRIMER RUKOVALAC – STANARI / VLASNICI
Kada stanari (zakupci/vlasnici) zaključe ugovor sa operaterom video nadzora o instalaciji video nadzora, tada operator video nadzora deluje po nalogu stanara (zakupca/vlasnika). Naravno ne mora biti više lica, moguće je da samo i jedan stanar/vlasnik zaključi ovakav ugovor. Stanari (zakupci/vlasnici) odlučuju o svrsi video nadzora, kategorijama podataka (npr. slike), dužini čuvanja podataka, pa su oni rukovaoci za ovu obradu podataka.

PRIMER RUKOVALAC – POSREDOVANJE U SKLAPANJU POSLA
Firma XY sklopila je ugovor o posredovanju u sklapanju poslova i angažovanju novih radnika sa firmom Headhunter. Ugovorom o posredovanju je jasno definisano da je rukovalac firma XY, a obrađivač firma Headhunter koja deluje po nalogu firme XY. Firma Headhunter se nalazi u dvostrukoj ulozi: prema osobama koje traže posao ona je rukovalac, dok se kao posrednik nalazi u ulozi obrađivača u slučaju sa firmom XY kao i ostalim firmama po čijem nalogu radi kao posrednik. Osim toga firma Headhunter je operator platforme „posredovanje u zapošljavanju“, koja sortira odgovarajuće kandidate za posao, kojima može direktno da pristupi firma XY. Pored toga odvojeno Headhunter poseduje sopstvenu bazu podataka sa prijavama kandidata, koju koristi u ovu svrhu. Iz ovoga se može zaključiti da Headhunter pored ugovora o posredništvu sa firmom

[110] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje 1/2010 o pojmu rukovaoca i obrađivača*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, 00264/10/DE, WP 169, str. 15, 16, 17, 18.

[111] *Ibidem*, str. 39.

[112] *Ibidem*, str. 35.

[113] *Ibidem*, str. 26.

XY, predstavlja rukovalaca u pošto u posredovanju zajedno sa firmom XY kontroliše sam postupak posredovanja.[114]

PRIMER ZAJEDNIČKI RUKOVAOCI – E-GOVERNMENT PLATFORMA

Platforme E-uprave funkcionišu kao interfejs između građana i organa uprave. Platforma prikuplja zahteve građana i odgovara odgovarajućom dokumentacijom građanima. Sama platforma se može posmatrati kao rukovalac, pošto prikuplja podatke građana i odlučuje kome će biti prosleđeni podaci. Pored toga obrađuje i dokumente, koje čuva i kojima ima pristup ovim podacima.[115]

3.5.2. Zajednička obrada podataka više rukovalaca (čl. 26 OUZP)

„Zajednička obrada podataka od strane više rukovalaca" (zajednički ili solidarni rukovaoci) postoji shodno čl. 26 st 1. OUZP: „Ako dvoje ili više rukovalaca zajednički odrede svrhe i načine obrade, oni su zajednički rukovaoci obrade. Oni na transparentan način međusobnim dogovorom određuju svoje odgovornosti za poštovanje obaveza iz ove uredbe, naročito uzimajući u obzir ostvarivanje prava pojedinaca i dužnosti u pogledu pružanja informacija iz člana 13. i 14., osim ako obaveze rukovaoca nisu utvrđene pravom Unije ili pravom države članice kojem rukovaoci obrade podležu. Dogovorom se može odrediti konkretno mesto za ostvarivanje prava pojedinca".

Pre nego što pređemo na detaljnu analizu samog čl. 26 OUZP potrebno je ustanoviti: Da li o svrhama i sredstvima obrade podataka o ličnosti odlučuje jedna ili više osoba (preduzeća, tela javnih vlasti)? (videti pojam rukovalac drugi element). Ovo pitanje proizlazi i iz prve rečenice čl. 26 st. 1 OUZP. Pritom i minimalan doprinos u određivanju sredstava i ciljeva obrade podataka može ustanoviti odgovornost.[116]

PRIMER GDE NE POSTOJE ZAJEDNIČKI RUKOVAOCI – PRENOS PODATAKA RADNIKA PORESKIM ORGANIMA

Po pravilu u većini država su firme dužne shodno zakonu da proslede podatke svojih zaposlenih u cilju obračuna poreza na zarade, socijalnog osiguranja. U ovom slučaju kada firma XY prosledi podatke svojih zaposlenih, iako i firma XY i poreski organi obrađuju identične podatke, oni *ne obrađuju ove podatke uz pomoć identičnih sredstava i nemaju identičnu svrhu obrade ovih vrsta podataka*. Stoga su firma XY i poreski organ odvojeni rukovaoci.[117]

[114] *Ibidem*, str. 23.

[115] *Ibidem*, str. 26.

[116] *Ibidem*, str. 16.

[117] *Ibidem*, str. 25.

PRIMER ZAJEDNIČKI RUKOVAOCI – BANKA I FIRMA ZA NAPLATU POTRAŽIVANJA
Ukoliko jedna banka za sporovođenje naplate svojih potraživanja prema klijentima angažuje firmu/agenciju za naplatu potraživanja. Pritom se banka i agencija slože oko sredstva i obrade finansijskih podataka klijenata. Dogovorom je regulisano da banka odlučuje kada će se vršiti sama naplata potraživanja prema klijentima a da tek u poslednjoj fazi dođe do same naplate potraživanja od strane agencije. Iako oba aktera i banka i agancija imaju svoje odvojene aktivnosti, oni su u poslednjoj fazi „fazi naplate potraživanja“ usko povezani i svrhom i sredstvima. U tom slučaju bi oni mogli biti posmatrani kao zajednički rukovaoci.[118]

Druga rečenica čl. 26 st. 1 OUZP govori o *obavezama pri zajedničkoj obradi podataka od strane više rukovalaca*.

U te obaveze spadaju:

- ✓ Zaključenje ugovora
- ✓ Izuzetak od zaključenja ugovora *(„otvorena klauzula“)*
- ✓ Transparentnost
- ✓ Centralno kontaktno mesto (opciono)
- ✓ Ostvarivanje prava pojedinaca

Zaključenje ugovora: Iako se saglasnost volja može postići na različite načine, indicija je da se *međusobna odgovornost rukovaoca reguliše pisanim sporazumom ili ugovorom*. Ovaj ugovor treba da sadrži:

- ✓ *Definisanje obaveza* (OUZP u čl. 26. st. 1 reguliše ispunjenje prava pojedinaca kao i dužnosti u pogledu pružanja informacija iz čl. 13 i 14 OUZP). Svakako da je potrebno detaljno regulisati ciljeve, način obrade podataka, evidenciju obrade podataka (čl. 30 OUZP), tehničke i organizacione mere (čl. 32 OUZP), procenu uticaja u vezi sa zaštitom podataka (čl. 35 OUZP).
- ✓ *Objašnjavanje funkcionisanja i veza*. Potrebno je ugovorom regulisati i međusovno objasniti vezu i funkcionisanje između rukovalaca (čl. 26 st. 2 OUZP). Takođe ovaj *ugovor mora biti dostupan pojedincima* (da li se radi o koncernu, akcionom društvu i uopšte o kojoj formi međusobne veze rukovalaca).

Neke delove nije moguće regulisati ugovorom, jer ih je OUZP već predvideo. Tako npr. shodno čl. 26 st. 3 OUZP mogu *pojedinci svoja prava ostvariti prema bilo kom rukovaocu*. Isto tako je u čl. 82 st. 2 OUZP regulisano da *svaki rukovalac odgovara za celokupnu štetu* (solidarna odgovornost rukovaoca), koja je prouzrokovana prilikom zajedničke obrade podataka.

[118] *Ibidem*, str. 25.

Izuzetak od zaključenja ugovora („otvorena klauzula“) ugovora: Shodno čl. 26 st. 1 *ne postoji obaveza zaključenja ugovora ukoliko ta obaveza proizlazi iz propisa*: osim ako obaveze rukovalaca nisu utvrđene pravom Unije ili pravom države članice kojem rukovaoci obrade podležu. U ovom slučaju se zahteva striktno regulisanje, kom rukovaocu je dodeljena koja obaveza. Ukoliko je regulisana zajednička obrada podataka više rukovaoca, a nisu raspodeljene obaveze, tada je neophodno sačiniti ugovor.

Transparentnost: Ugovor bi trebalo da bude sačinjen zbog lakšeg dokazivanja u pisanoj formi. Transparentnost se ogleda u tome da ugovor treba da bude dostupan nadzornom organu za zaštitu podataka ali i pojedincima (čl. 26 st. 2 OUZP). Nije neophodno da se čitav sadržaj ugovora učini dostupnim, već *informacije koje su od suštinskog značaja za pojedince*. Samim tim se može reći da su to informacije koje su isključivo od značaja za obradu podataka, a koje su i obuhvaćene *članovima 13 i 14 OUZP*.

Centralno kontaktno mesto (opciono): Dogovorom se može odrediti kontaktno mesto za ostvarivanje prava pojedinca (čl. 26 st. 1 OUZP). Ova mogućnost je ostavljena rukovaocima da sami odrede, ukoliko žele. Postoji više načina kako bi to centralno kontantno mesto moglo da funkcioniše:

- ✓ Centralno kontantno mesto bi moglo da bude odgovorno za rešavanje pitanja prava pojedinaca.
- ✓ Centralno kontantno mesto bi moglo da bude odgovorno da prosledi odgovornom rukovalacu zahteve za rešavanje prava pojedinaca.
- ✓ Centralno kontantno mesto bi moglo da imenuje odgovorne za rešavanje prava pojedinaca.

Ostvarivanje prava pojedinaca: Kao što je već istaknuto *nezavisno od samog ugovora pojedinac ima pravo da ostvari svoja prava prema svim rukovaocima.* Razloge u ovakvoj odredbi treba tražiti pre svega u osnaživanju prava pojedinaca, ali i u onemogućavanju rukovaoca da se kriju iza neregulisane odgovornosti.[119]

PRIMER ZAJEDNIČKI RUKOVAOCI – PORTAL ZA PUTOVANJA
Turistička agencija, hotelski lanac i avio kompanija su napravili zajedničku internet platformu u cilju upravljanja rezervacijama putovanja. Ugovorom su regulisali sredstva – koji podaci će biti čuvani, kako će se rezervacije odvijati i ko će imati pristup podacima. Regulisali su takođe da se podaci putnika zajednički koriste kao i reklamne kampanje. Pošto sve tri kompanije u lancu imaju kontrolu podataka putnika preko internet platforme, za ovu obradu podataka oni su zajedički rukovaoci u smislu OUZP. U pogledu ostalih obrada podataka oni i dalje imaju odgovornost rukovalaca.[120]

[119] Bernhard Horn, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 158, 159, 160, 161, 162, 163.

[120] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje 1/2010 o pojmu rukovaoca i obrađivača*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, 00264/10/DE, WP 169, str. 24.

Kod *odgovornosti pri zajedničkoj obradi podataka od strane više rukovalaca* (čl. 82 st. 4 OUZP) regulisano je da *svaki rukovalac odgovara za celokupnu štetu* (solidarna odgovornost rukovaoca), koja je prouzrokovana prilikom zajedničke obrade podataka. Pritom oštećenom stoji slobodno na raspolaganju prema kome će postaviti zahtev za naknadu štete (čl. 26 st. 3 OUZP). Rukovalac koji namiri dug, može se naplatiti od ostalih rukovaoca srazmerno visini duga. Na taj način je omogućeno *pravo regresa rukovaoca koji isplati dug* (čl. 83 st. 5 OUZP).

Neki od rukovaoca pri zajedničkoj obradi može se *osloboditi odgovornosti*, ako *dokaže da nije ni na koji način odgovoran za događaj koji je prouzrokovao štetu* (čl. 83 st. 3 OUZP). Teret dokazivanja je na rukovaocu.

3.5.3. Obrađivač (čl. 4 br. 8 OUZP) i prava i obaveze (čl. 28 OUZP)

Definicija

„Obrađivač" je fizičko ili pravno lice, telo javne vlasti, agencija ili drugo telo koje obrađuje podatke o ličnosti u ime rukovalaca.

Sama definicija je takođe preuzeta iz Direktive o zaštiti podataka 95/46/EC.[121] Moderno doba sa sobom nosi jedan trend u kome su usluge obrađivača sve traženije. Danas se usluge autsorsuju (eng. outsourcing) odnosno prenose kompletno obrađivačima, takođe usluge klauda (eng. cloud services) i industrija 4.0. su samo od nekih usluga koje uglavnom obavljaju obrađivači.

Mora se naglasiti da je *obrađivač u lancu odgovornosti zaštite podataka samo mogućnost i stvar izbora rukovalaca*. Dakle obrađivač nije nužni učesnik u obradi podataka o ličnosti, pošto rukovalac može deo ili čitavu obradu podataka preneti obrađivaču (spoljnom ili eksternom pružaocu usluga). Pritom je od suštinskog značaja da *obrađivač deluje u ime i isključivo po nalogu rukovaoca* (čl. 29 OUZP). Uz to obrađivač *ne sme odlučivati o svrsi i sredstvima obrade podataka*. Iako je i za ovu obavezu predviđena *„otvorena klauzula"* (mogućnost da se drugačije reguliše ovo pitanje pravom Unije ili pravom države članice), može se reći da je obrađivač dužan da ispunjava naloge rukovaoca pogotovu u pogledu cilja i sredstva obrade podataka. Ipak i ta obaveza daje obrađivačima *mogućnost da izaberu odgovarajuće tehničke i organizacione mere, a da pritom ne promene uloge. Ukoliko pak obrađivači prekorače svoju ulogu* i preuzmu ulogu odlučivanja o svrsi i sredstvima obrade podataka, tada *njih treba tretirati kao zajedničke rukovaoce*.[122] Shodno čl. 28 st. 10 OUZP ukoliko obrađivač krši ovu uredbu utvrđivanjem svrhe i načina obrade podataka, obrađivač

[121] Isto kao i za termin rukovalac, termin obrađivač je manjkav. U Hrvatskoj je u upotrebi termin izvršitelj obrade, takođe se mogu koristiti termini kao što su nalogoprimac, serviser, upravljač podacima po nalogu, odgovorno lice za obradu po nalogu.

[122] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje 1/2010 o pojmu rukovaoca i obrađivača*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 00264/10/DE, WP 169, str. 31.

se smatra *rukovaocem* u pogledu te obrade. Sa stanovišta pojedinca/pogođenog lica svakako se radi o zajedničkim rukovaocima, koji bi trebalo da solidarno odgovaraju.

Izuzetno važno za organizacije je da one mogu imati *više uloga, kako ulogu rukovaoca, tako i ulogu obrađivač*a zavisno od konkretne obrade podataka. Kakav će status biti, potrebno je proceniti u zavisnosti od okolnosti i konkretne obrade podataka.

PRIMER OBRAĐIVAČ – VEB HOSTING USLUGE I SERVER HOUSING USLUGE
Ponuđači veb hosting usluga treba generalno klasifikovati kao obrađivače. Oni nude klijentima hosting (najčešće se misli na veb sajt, koji uključuje bazu podataka sa aplikacijama), održavanje veb sajta. Ukoliko bi ponuđači ovih usluga koristili podatke klijenata u sopstvene svrhe, tada i oni deluju kao rukovaoci. Ponuđači usluga „server hosting“ su takođe generalno obrađivači. IT infrastruktura je na taj način smeštena na odgovarajuće računarske centre sa adekvatnim kvalitetom i najvišim standardima bezbednosti.

PRIMER OBRAĐIVAČ – PORESKI SAVETNIK/KONTROLOR RAČUNA
Uglavom ponuđači usluga poreskog savetovanja ili kontrolisanja računa nude obe usluge. Sa stanovišta zaštite podataka ukoliko kontolišu račune npr. u cilju sačinjavanja poreske prijave onda oni istupaju kao rukovaoci (kao i advokati, notari itd.). Ukoliko se usluga odnosi na kontrolisanje knjigovodstva i striktinim nalozima rukovaoca, tada bi se moglo reći da se radi o obrađivaču, jer se ne radi o zaposlenom unutar neke firme. Međutim ukoliko poreski savetnik konstatuje da je neophodna prijava poreza, tada on postupa po osnovu svojih dužnosti i tada se on može klasifikovati kao rukovalac.[123]

Ustanovljavanje obrađivača

Da bi postojao obrađivač neophodno je da su ispunjena dva preduslova:

- ✓ Da je obrađivač nezavisno lice (pravno ili fizičko)
- ✓ Da obrađuje podatke u ime i po nalogu rukovaoca (čl. 29 i čl. 28. st. 3 a) OUZP) shodno sačinjenom ugovoru (čl. 28 st. 3 OUZP).[124]

Ugovor između rukovaoca i obađivača treba da bude *sačinjen u pisanoj ili elektronskoj formi* (čl. 28 st. 9 OUZP).

Ugovor može biti zaključen:

- ✓ Na osnovu sporazuma rukovaoca i obrađivača; ili
- ✓ Standardnih ugovornih klauzula EU (čl. 28 st. 7 OUZP); ili
- ✓ Standardnih ugovornih klauzula nacionalnih institucija za zaštitu podataka (čl. 28 st. 8 OUZP); ili

[123] *Ibidem*, str. 35.

[124] *Ibidem*, str. 30.

- ✓ Drugih pravnih instrumenata (verovatno se misli na zakon ili uredbu – videti čl. 28 st. 9 OUZP).

Ugovor mora da sadrži sledeće odredbe (čl. 28 st. 3 OUZP):

- ✓ Predmet ugovora i trajanje obrade podataka;
- ✓ Vrstu i svrhu obrade;
- ✓ Kategorije podataka o ličnosti;
- ✓ Kategorije pogođenih pojedinaca;
- ✓ Prava i obaveze rukovaoca;
- ✓ Obavezu obrađivača, da obrađuje podatke u ime i po dokumentovanom nalogu rukovaoca;[125]
- ✓ Obavezu obrađivača, da ovlašćene osobe za obradu podataka o ličnosti obaveže na poštovanje tajnosti podataka ili da podležu zakonskim obavezama o tajnosti podataka:
- ✓ Obavezu obrađivača, da implementira sve neophodne organizacione i tehničke mere u cilju bezbednosti podataka iz čl. 32 OUZP;
- ✓ Obavezu obrađivača, da pomogne rukovaocu tehničkim i organizacionim merama u ispunjenju prava pojedinaca iz poglavlja III;
- ✓ Obavezu obrađivača, da pomogne rukovaocu u sprovođenju obaveza predviđenih u članovima 32-36 OUZP (to su mere za bezbednost podataka, izveštavanje nadzornog organa za zaštitu podataka ili pojedinaca pri povredi bezbednosti podataka, procena uticaja u vezi sa zaštitom podataka, predhodna konsultacija nadzornog organa za zaštitu podataka);
- ✓ Obavezu obrađivača, da nakon završetka ugovora sve podatke o ličnosti po izboru rukovaoca ili obriše ili vrati, osim ako čuvanje podataka nije regulisano pravom EU ili država članica „otvorena klauzula“;
- ✓ Obrađivač je dužan, da stavi rukovaocu na raspolaganje sve informacije koje su neophodne za dokazivanje poštovanja obaveza utvrđenih ugovorom u cilju obavljanja revizije ili inspekcije;
- ✓ Obrađivač je takođe dužan, da stavi rukovaocu na znanje da su njegovi nalozi protivpravni nezavisno od ugovornih klauzula i da ukaže na mogući pravni prestup.

Pored odredaba koje mora da sadrži svaki ugovor, moguće je naravno ugovoriti i dodatne klauzule, kao i dodatno razjasniti navedene.

[125] U pogledu davanja dokumentovanih naloga predviđena je mogućnost *„otvorene klauzule“,* ako je regulisano drugačije pravom EU ili pravom države članice EU. Tada je obrađivač dužan da obavesti o tome rukovaoca pre same obrade podataka, ako i samo obaveštenje nije iz razloga javnog interesa isključeno tim pravnim osnovom (čl. 28 st. 3 a) OUZP).

Načela obrade podataka i zakonitost obrade obrađivača

Obađivača obavezuju takođe načela obrade podataka (čl. 5 OUZP). Ovo se posebno odnosi na one obrađivače koji određuju bližu upotrebu sredstava obrade.

U pogledu zakonitosti i sama dopuštenost obrade podataka važi takođe za obrađivače (čl. 6 OUZP). To podrazumeva da bi uopšte došlo do angažovanja obrađivača i da bi on mogao da obavllja aktivnosti obrade, neophodno je da postoji neki od zakonskih osnova obrade podataka.[126]

Tako je primera radi pri prikupljanju podataka pojedinaca radi obrade podataka u okviru koncerna neophodno je pre same obrade da pojedinac da pristanak na obradu podataka i od obrađivača (čl. 6 st. 1 a) OUZP).

Posebni uslovi dopuštenosti predviđeni su za prenos podataka u treće zemlje. Ovi uslovi važe i za obrađivača prilikom transfera podataka u treće zemlje.

Osim toga treba istaći da se *norme OUZP odnose na obrađivače koji imaju svoje sedište u EU* ali *i na one koji to nemaju*. Od važnosti je da *se roba i usluge nude u EU ili* se *obrada podataka odnosi na praćenje ponašanja pogođenih lica u EU*. Ukoliko *obrađivač nema na sedište u EU* on je dužan da imenuje u pisanoj formi (čl. 27 OUZP) *predstavnika u EU*, koji može biti fizičko ili pravno lice (čl. 4 tč. 17 OUZP).

Obaveze rukovaoca pri izboru obrađivača

U pogledu *izbora obrađivača*, rukovalac je u obavezi da izabere takvog obrađivača, koji će ponuditi dovoljne *garancije* u vidu *odgovarajućih tehničkih i organizacijskih mera pre svega u cilju zaštite prava pojedinaca* (videti čl. 28 st. 1 OUZP). Kao *kriterijumi za procenu podobnih obrađivača* mogu se uzeti:

- ✓ stručno znanje,
- ✓ pouzdanost,
- ✓ resursi,
- ✓ sprovođenje tehničkih i organizacionih mera pre svega u pogledu sigurnosti obrade podataka (U.t.r. 81 OUZP).

Osim navedenih kriterijuma kao dokaz pouzdanosti obrđivača mogu se uzeti i *odobren kodeks ponašanja* (čl. 40 OUZP) *ili odobren postupak sertifikacije* (čl. 42 OUZP).

Angažovanje više obrađivača (sub-obrađivača)

Danas je veoma česta situacija u praksi da rukovalac *angažuje više obrađivača ili da obrađivač angažuje obrađivača (sub-obrađivača)*, kojima se poveravaju različite aktivnosti u obradi podataka. U svakom slučaju svi akteri u lancu su *dužni da slede naloge rukovaoca*.

[126] Rene J. Bogendorfer, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 172, 173, 174.

U pogledu regulisanja ugovorom oko angažovanja *novih obrađivača (sub-obrađivača)* postoje sledeće mogućnosti:

- ✓ da rukovalac daje ugovorno *opšti pisani pristanak* na angažovanje drugih obrađivača; ili
- ✓ da rukovalac mora da da *posebno odobrenje* za angažovanje drugih obrađivača.

Ako je ugovorom regulisano opšte pisano odobrenje za angažovanje drugih obrađivača, onda rukovalac *mora biti obavešten o svakoj daljoj nameri angažovanja obrađivača i može da uloži prigovor* na to da obrađivač prenese određene aktivnosti nekom novom obrađivaču (čl. 28 st. 2 OUZP).

Ugovor sa sub-obrađivačom treba sačiniti u *pisanoj ili elektronskoj formi* (čl. 28 st. 9 OUZP). Ovim ugovorom treba regulisati *identične obaveze za sub-obrađivača kao što ih je imao obrađivač* (čl. 28 st. 4 OUZP). Isto tako *u pogledu izbora sub-obrađivača važe identična pravila kao i za izbor obrađivača*. Misli se pre svega na tehničke i organizacione mere kao i kriterijume za pouzdanost sub-obrađivača. Ukoliko sub-obrađivač ne ispunjava adekvatno svoje obaveze, *rukovaocu odgovara direktno obrađivač* (čl. 28 st. 4 OUZP).

Obaveza vođenja evidencije obrade podataka

Obrađivač (kao i njegov zastupnik, ako se radi o obrađivaču van EU) ima jednu posebnu obavezu koja bi takođe morala da bude regulisana navedena i ugovoru a to je skraćeno *vođenje evidencije obrade podataka* (čl. 30 st. 2 OUZP). Radi se o skraćenoj varijanti u odnosu na rukovaoce u smislu manje količine informacija, koje evidencija obrade podataka treba da sadrži.

Evidencija obrade podataka obrađivača treba da sadrži (čl. 30 st. 2 OUZP):

- ✓ ime i kontakt podatke jednog ili više obrađivača i svakog rukovaoca po čijem nalogu obrađivač deluje, i ako je primenljivo, zastupnika rukovaoca ili obrađivača kao i ovlašćenog lica za zaštitu podataka;
- ✓ kategorije podataka koje se obavljaju u ime svakog rukovaoca;
- ✓ ako je primenjivo, prenos podataka o ličnosti u treće zemlje ili međunarodne organizacije, uključujući identifikaciju treće zemlje ili međunarodne organizacije kao i u slučaju prenosa iz člana 49. stav 1. tačke (h), dokumentaciju o odgovarajućim zaštitnim merama;
- ✓ ako je moguće, opšti opis tehničkih i organizacionih bezbednosnih mera iz člana 32. stav 1.

Evidencija obrade mora se voditi u *pisanoj formi ili elektronskoj formi* (čl. 30 st. 3 OUZP).

Izuzetci od obaveze vođenja evidencije (čl. 30 st. 5 OUZP) obrade podataka za obrađivača predviđeni su:

- ✓ ako firma ili organizacija ima manje od 250 zaposlenih i ako obrada podataka ne predstavlja visok rizik za prava i slobode pojedinaca; i
- ✓ ako je obrada podataka povremena *ili* ne uključuje posebne kategorije podataka iz člana 9. stav 1. *ili* podatke o krivičnim presudama i krivičnim delima iz člana 10.

Obrađivač (kao i njegov zastupnik) dužni su da *na zahtev daju evidenciju obrade podataka instituciji za zaštitu podataka* (čl. 30 st. 4 OUZP).

Obaveza imenovanja ovlašćenog lica za zaštitu podataka za obrađivače

U pogledu *obaveze imenovanja ovlašćenog lica za zaštitu podataka* (eng. data protection officer) i za obrađivača postoji identična obaveza kao i za rukovaoca.

Obrađivač je u obavezi da imenuje ovlašćeno lice za zaštitu podataka, ukoliko su ispunjeni sledeći uslovi (čl. 37 OUZP):

- ✓ obradu podataka vrši telo *javne vlasti ili javno telo*, osim za sudove koji deluju u okviru svoje sudske nadležnosti, ili
- ✓ *osnovne delatnosti obrađivača* se sastoje od postupaka obrade koji zbog svoje *prirode, obima i/ili svrha iziskuju redovno i sistematično praćenje pojedinaca* u velikoj meri, ili
- ✓ *osnovne delatnosti obrađivača* se sastoje od opsežne obrade *posebnih kategorija podataka* na osnovu člana 9. i podataka o ličnosti u vezi sa *krivičnim osudama i krivičnim delima* iz člana 10.

O tome *šta je osnovna delatnost*, tumačenje nam daje U.t.r. 97 OUZP: „U privatnom sektoru, osnovne delatnosti rukovalaca se odnose se njegove primarne delatnosti i ne odnose se na obradu podataka o ličnosti kao sporedne delatnosti.“. Da se primetiti da OUZP na ovom mestu govori samo o rukovaocima, ali svakako da bi to trebalo primeniti i na obrađivače.

PRIMER OSNOVNA DELATNOST – BOLNICE
Osnovna delatnost bolnice se sastoji u pružanju zdravstvene nege. Da bolnice ne obrađuju zdravstvene podatke svojih pacijenata, ne bi bili u mogućnosti da obavljaju svoju osnovnu delatnost. Stoga je se obrada ovakvih podataka može smatrati kao osnovna delatnost u smislu OUZP, pa su bolnice dužne da angažuju ovlašćeno lice za zaštitu podataka.[127]

[127] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Vodič u vezi sa ekspertima za zaštitu podataka*, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), 16/DE, WP 243, str. 8

PRIMER OSNOVNA DELATNOST – AGENCIJA ZA NADZOR

Osnovna delatnost agencije ili firme koje se bavi nadzorom sastoji se u nadzoru objekata, lica. Ova osnovna delatnost se ne može odvojiti od obrade podataka o ličnosti. Stoga su takođe firme, koje se bave nadzorom u obavezi da angažuju ovlašćeno lice za zaštitu podataka.[128]

PRIMER KADA NE POSTOJI OSNOVNA DELATNOST
Osnovna delatnost ne postoji kod nagrađivanja zaposlenih ili kod usluga standardnih IT-support servisa. Ovde se radi o tome da se osnovna delatnost ovih firmi odnosi na pomoćne delatnosti. Iako ove aktivnosti mogu biti od izuzetnog značaja za neku firmu, one u smislu OUZP predstavljaju sporedne delatnosti.[129]

Odgovornost obrađivača

U pogledu *odgovornosti obrađivač* odgovara kako građansko pravno tako i upravno pravno. Upravno pravno on odgovara za prouzokovanu štetu, kada je *postupao suprotno dodeljenim obavezama ili nije sledio naloge rukovaoca* (čl. 82 st. 2 OUZP). Obrađivač se može osloboditi ove odgovornosti, ako dokaže da nije ni na koji način odgovoran za događaj koji je prouzrokovao štetu (čl. 82 st. 3 OUZP). Ako su u šteti učestvovali i rukovalac i obrađivač u okviru iste obrade podataka i ukoliko se pokaže njihova odgovornost, tada oni odgovaraju *solidarno* (čl. 82 st. 4 OUZP). Ukoliko je rukovalac ili obrađivač isplatio celokupnu štetu, onom ko je isplatio pripada *pravo regresa* u odnosu na isplaćenu naknadu štete (čl. 82 st. 5 OUZP).

[128] *Ibidem*.

[129] *Ibidem*.

4. OSNOVNA NAČELA I ZAKONITOST OBRADE PODATAKA

4.1. Načela obrade podataka

Načela obrade podataka su pored zakonitosti obrade (čl. 6 OUZP) od suštinskog značaja za usaglašenost rukovaoca i obrađivača sa OUZP. Svaka aktivnost obrade podataka treba da bude u skladu sa načelima zaštite podataka. Poštoje 6 načela zaštite podataka i jedno supra-načelo, načelo društvene odgovornosti „načelo o načelima". Načela zaštite podataka iako predstavljaju osnovne principe zaštite podataka, svoja ostvarenja i konkretizaciju nalaze u normama OUZP.

4.1.1. Načelo zakonitosti, poštenja i dobrih običaja, transparentosti (čl. 5 st. 1 a) OUZP)

U ovo načelo je pored uslova da podaci moraju biti obrađivani zakonito i pravično, uključena i transparentnost kao jedan od osnovnih aspekata ovog principa. *Transparentnost* je nerazdvojno povezana sa pravednošću i načelom društvene odgovornosti prema OUZP.

Veza transparentnosti i društvene odgovornosti se zasniva na tome da je rukovalac u obavezi da dokaže da su lični podaci obrađivani na transparentan način u odnosu na pojedinca (čl. 5 st. 2 OUZP). Princip društvene odgovornosti zahteva transparentnost operacija obrade kako bi rukovaoci mogli da dokažu poštovanje svojih obaveza prema OUZP. *Pridržavanjem načela transparentnosti od strane rukovaoca omogućava se pojedincima da spoznaju odgovornost rukovaoca i obrađivača, kao i da efektivno vrše kontrolu nad svojim ličnim podacima.* Npr. davanje ili povlačenje pristanka pojedinaca i provera delotvornost njihovih prava.

Jedan od bitnih zahteva načela transparentnosti je da *pojedinac treba da bude u stanju da unaped utvrdi obim i posedice obrade*, *da se ne bi iznenadio* u toku obrade o načinima na koji su korišćeni njegovi podaci. Ovaj zahtev je takođe *važan aspekt principa pravičnosti* (čl. 5 st. 1 i U.t.r. 39 OUZP). Shodno ovom zahtevu „pojedinci bi trebalo da budu upoznati sa rizicima, propisima, zaštitnim merama i pravima u vezi sa obradom podataka o ličnosti...". Kod složene, tehnički ili neočekivane obrade podataka i kod pružanja informacija shodno čl. 13 i 14 OUZP, rukovaoci treba da jasno objasne u pisanoj formi koje su to najvažnije posledice obrade. Pojedincima treba objasniti, kakav će efekat po njih imati specifična obrada opisana u izjavi o privatnosti / obaveštenju. Osim toga u slučaju npr. računarstva u oblacima neophodno je korisnicima "cloud-a" pružiti dodatne informacije o primaocima ili kategorijama podataka koje obrađuju primaoci, koji mogu uključiti i obrađivače i podobrađivače. Pružanjem ovih informacija osigurava se pravičnost prema pojedincima.[130] U skladu

[130] Radna grupa član 29, Datenschutzgruppe Artikel 29, *Mišljenje 05/2012 o računarstvu u oblacima*, Stellungnahme 05/2012 zum Cloud Computing, 01037/12/DE, WP 196, 1.7.2012, str. 13.

sa načelom društvene odgovornosti i u skladu sa U.t.r. 39 OUZP, rukovaoci bi trebalo da procene da li postoje posebni rizici za fizička lica uključeni u obradu, na koje treba obratiti posebnu pažnju pojedincima. [131]

Načelo transparentnosti primjenjuje se bez obzira na pravnu osnovu obrade podataka i *tokom celog životnog ciklusa obrade podataka*. Prema čl. 12 OUZP transparentnost se primjenjuje u sledećim fazama ciklusa obrade podataka:

- ✓ pre ili na početku ciklusa obrade podataka, tj. kada su lični podaci prikupljeni ili od pojedinca ili dobijeni na drugi način;
- ✓ tokom celog perioda obrade, tj. kada se komunicira sa pojedincima o njihovim pravima; i
- ✓ o određenim temama dok obrada traje, npr. kada dođe do povrede bezbednosti podataka ili u slučaju promena u obradi.[132]

Značenje transparentnost nije definisano u samom tekstu OUZP, već je pomereno u uvodne tačke razmatranja uredbe. U.t.r. 39 OUZP objašnjava značenje i efekat principa transparentnosti u kontekstu obrade podataka:

"Za pojedince bi trebalo biti transparentno kako se podaci koji se odnose na njih prikupljaju, koriste, daju na uvid ili na drugi način obrađuju, kao i do koje se mere ti podaci obrađuju ili će se obrađivati. Načelom transparentnosti traži se da svaka informacija i komunikacija u vezi sa obradom tih podataka bude *lako dostupna i razumljiva i da se upotrebljava jasan i jednostavan jezik*. To načelo se naročito odnosi na informacije koje se daju pojedincu o identitetu rukovaoca i svrhama obrade kao i ostale informacije radi osiguravanja poštenja i transparentnosti obrade s obzirom na pojedince o kojima je reč i njihovom pravu da dobiju potvrdu i na obaveštenje (informaciju) o ličnim podacima koji se obrađuju, a koji se odnose na njih…".

Važan preduslov (čl. 12 st. 5 OUZP) ostvarivanja načela transparentnosti je da *rukovaoci ne mogu generalno da naplaćuju pružanje informacija* (čl. 13 i 14, 15-22 i 34 OUZP). Svaka informacija koja se pruža u skladu sa zahtevima transparentnosti ne može biti uslovljena finansijskim transakcijama (npr. plaćanjem ili kupovinom robe ili usluga).[132]

Zajednički rukovaoci treba da omoguće pojedincima informacije iz čl. 13 i 14 OUZP na transparentan način i u pogledu ostvarivanja njihovih prava (čl. 26 st.1 OUZP). Od zajedničkih rukovaoca se zahteva da predoče pojedincima suštinu njihovog međusobnog dogovora (čl. 26 st. 2 OUZP). Pojedincima mora biti potpuno jasno na koji način i kod kog rukovaoca mogu ostvariti svoja prava.[134]

---

[131] Radna grupa član 29, Article 29 Working Party, *Vodič u vezi sa transparentnošću pod OUZP*, Guidelines on transparency under Regulation 2016/679, 17/EN, WP260 rev.01, 11.4.2018, str. 5, 7.

[132] *Ibidem*, str. 6.

[133] *Ibidem*, str. 13.

[134] *Ibidem*, str. 22.

Vršenje prava subjekata podataka je vezano za načelo transparentnosti. U tom pogledu je rukovalac u obavezi da pojedinacu:

- ✓ pruži informacije pojedincima o njihovim pravima (čl. 13 st. 2 b) i ćl. 14 st. 2 c) OUZP);
- ✓ poštuje princip transparentnosti i kvalitet komunikacije (lak, razumljiv jezik) kada komunicira sa pojedincima u vezi sa njihovim pravima (čl. 15-22 i 34 OUZP);
- ✓ olakša ostvarivanje prava pojedinaca u skladu sa čl. 15 do 22 OUZP (U.t.r. 59 OUZP).

PRIMER OMOGUĆAVANJE OSTVARIVANJA PRAVA POJEDINACA
Zdravstvena ustanovana svom veb sajtu koristi elektronski obrazac i papirne formulare pri prijemu u bolnicu, kako bi se olakšalo podnošenje zahteva. Zdravstvena ustanova prihvata i zahteve koji su podneseni na drugi način (npr. pismom, e-mailom) i pruža posebnu mogućnost za kontaktiranje (kojoj se može pristupiti putem e-maila i putem telefona) kako bi se pomoglo pojedincima u ostvarivanju njihovih prava.[135]

Najvažniji element načela transparentnosti se odnosi na prava pojedinca, koja se nalaze u Poglavlju III (prava pojedinaca). Čl. 12 OUZP reguliše opšta pravila koja se primenjuju pružanje informacija pojedincima; pružanje informacija pojedincima (čl. 13 i 14 OUZP); komunikacije sa pojedincima o ostvarivanju njihovih prava (čl. 15-22 OUZP); komunikacija u vezi sa zloupotrebom podataka (čl. 34 OUZP). O ovim pravima pojedinaca biće govora u narednim poglavljima.

4.1.2. Načelo vezanosti za svrhu obrade podataka (čl. 5 st. 1 b) OUZP)

Jedno od najznačajnijih načela zaštite podataka o ličnosti jeste *načelo vezanosti za svrhu obrade podataka.* Obrada podataka je ograničena na posebnu, određenu i zakonitu svrhu, koja je utvrđena pri prikupljanju podataka. Tako se podaci generalno obrađuju u različite svrhe – npr. izvršenje ugovora, marketing, knjigovođstvo, isplata zarada zaposlenima. Sama obrada podataka je dakle vezana za svrhu obrade.

U ovom kontekstu treba razlikovati *„prikupljanje"* podataka (prvobitno ili inicijalno prikupljanje) i *„dalju obradu"* (nova obrada, koja odstupa od prvobitne) podataka. *Kod dalje obrade podataka* je generalno neophodno *proveriti usklađenost prvobitne obrade podataka sa novom obradom podataka*.

4.1.3. Načelo smanjenja (minimizacije) količine podataka (čl. 5 st. 1 c) OUZP)

Načelo smanjenja (minimizacije) količine podataka (čl. 5 st. 1 c) OUZP) se odnosi na to da podaci o ličnosti treba da budu *poroporcionalno određeni, neophodni*

[135] *Ibidem*, str. 25, 26.

i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju. Ovo načelo se sastoji dakle iz 3 ključna elementa:

- ✓ Proporcionalnost obrade podataka;
- ✓ Neophodnost obrade podataka;
- ✓ Nužnost obrade podataka.

Proporcionalnost je potvrđena, ukoliko je obrada podataka u njenom obimu srazmerna.[136] Kod *neophodnosti* obrade podataka treba se zapitati, da li je obrada podataka pogodna da bi se uz pomoć takve obrade podataka postigao legitimni cilj (svrha). Pitanje *nužnosti* se u ovom kontekstu odnosi na to da li je nužno obrađivati određenu količinu podataka ili se cilj može postići sa obradom manje količine podataka.[137] To podrazumeva i da rok čuvanja podataka bude ograničen na apsolutni minimum. Takođe pri oceni nužnosti treba imati u vidu da *podatke o ličnosti treba obrađivati samo ako se svrha obrade opravdano ne bi mogla postići drugim sredstvima* (U.t.r. 39 OUZP).

4.1.4. Načelo tačnosti podataka (čl. 5 st. 1 d) OUZP)

Podaci o ličnosti moraju da budu tačni i ažurirani. Potrebno je preduzeti adekvatne mere da netačni podaci budu bez odlaganja obrisani ili ispravljeni (čl. 16 OUZP).

Osim toga načelo tačnosti podataka pojašnjava i U.t.r. 39 OUZP „Treba preduzeti sve potrebne korake da se obezbedi da se netačni podaci o ličnosti isprave ili obrišu". Ovo načelo takođe predpostavlja primenu adekvatnih tehničkih i organizacionih mera (čl. 32 OUZP), kako bi se podaci redovno ažurirali i ostali tačni.

4.1.5. Načelo ograničenog čuvanja podataka (čl. 5 st. 1 e) OUZP)

Podaci o ličnosti treba da budu čuvani u formi u kojoj je identifikacija pogođenih lica onoliko dostupna, koliko je to neophodno za ostvarivanje svrhe obrade podataka. To znači da rok čuvanja podataka o ličnosti traba da bude ograničen na najmanju moguću meru. Stoga rukovaoci da bi se obezbedilo da se podaci o ličnosti ne čuvaju duže nego što je neophodno, *treba da odrede rok za brisanje* ili *periodično*

---

[136] Kriterijumi za obim obrade podataka bi bili broj pojedinaca, količina obrađivanih podataka, vreme/ dužina trajanja obrade, geografski domašaj. Artikel 29 Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 4. April 2017 überarbeitet und angenommen am 4. Oktober 2017, 17/DE WP 248 Rev. 01, str. 11.

[137] Karsten Kinast, Themenreihe DSGVO: Grundsätze der Verarbeitung, 9. Juni 2017, https:// www. datenschutzticker.de /2017 /06/ themenreihe- dsgvo- grundsaetze-der-verarbeitung/, 20.06.2018.

kontrolisanje rokova čuvanja (U.t.r. 39 OUZP). To podrazumeva kreiranje *koncepta brisanja podataka*. Inače *podaci koji nisu potrebni za svrhe u koje su prikupljeni ili na drugi način obrađeni, treba da budu obrisani bez nepotrebnog odlaganja* (čl. 17 st. 1 a) OUZP).

Drugim rečima ako podaci više nisu potrebni treba da budu obrisani, a ukoliko postoje zakonski rokovi čuvanja podatke treba čuvati u zakonski predviđenom roku.

Čuvanje podataka u dužem periodu je uslovljeno sprovođenjem adekvatnih tehničkih i organizacionih mera *u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe u skladu sa članom 89 OUZP*.[138]

4.1.6. Načelo integriteta i poverljivosti podataka (čl. 5 st. 1 f) OUZP)

Ovo načelo služi ostverenju bezbednosti podataka i predstavlja 2 od 3 osnovna načela bezbednosti informacija. *Nedostaje* samo još *načelo dostupnosti* podataka, koje nije eksplicitno regulisano kao načelo.

Od izuzetnog značaja je da je bezbednost informacija odnosno podataka podignuta na rang načela zaštite podataka od ličnosti. Ostvarivanje ovog načela nalazimo u članu 32 OUZP „bezbednost obrade podataka".

Načelo integriteta (celovitosti) i poverljivosti podataka zahteva implementaciju *adekvatnih tehničkih i organizacionih mera zaštite*, pre svega da bi se sprečila *povreda bezbednosti podataka* (čl. 4 tč. 12 OUZP). Iako se kod načela zaštite podataka navodi „zaštita od neovlašćene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja" za razliku od definicije povrede bezbednosti podataka koji ima širi spektar zaštite „slučajno ili nezakonito uništenje, gubitak, izmena, neovlašćeno otkrivanje ili pristup podacima o ličnosti koji su preneti, uskladišteni ili na drugi način obrađivani". Može se primeniti da nedostaju u čl. 5 st. 1 f) OUZP delovi koji se tiču „izmene podataka, neovlašćenog otkrivanja ili pristupa podacima". Ovi delovi se inače odnose na načela integriteta – neovlašćene izmene podataka, odnosno poverljivosti i integriteta – ukoliko se podaci neovlašćeno otkrivaju ili im se neovlašćeno pristupa. Ovaj propust OUZP je više teorijsko-naučnog karatkera, ali ne i suštinske prirode. Stoga je bitno imati u vidu da tehničke i organizacione mere zaštite imaju svoju svrhu upravo u spečavanju povreda bezbednosti podataka u vidu primene adekvatnih tehničkih i organizacionih mera (čl. 32 OUZP).[139]

---

[138] Wirtschaftskammer Österreich, EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung, https:// www.wko.at/ service/ wirtschaftsrecht-gewerberecht/ EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html, 1.11.2018.

[139] Markus Kastelitz, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 104.

4.1.7. Načelo društvene odgovornosti (čl. 5 st. 2 OUZP)

Načelo društvene odgovornosti je novo načelo, koje je uvedeno donošenjem OUZP. Termin ovog načela je sporan zbog njegovog prevoda. Generalno on poručuje da je *odgovornost proverljiva i preuzeta (spoznata*). Odgovornost i društvena odgovornost su dve strane iste medalje, a obe se zapravo odnose na dobro upravljanje. Engleski pojam „Accountability" se može interpretirati kao „reinforced responsibility" pojačana odgovornost, „assurance" obezbeđivanje/garancija, „reliability" pouzdanost. Može se reći da se načelo društvene odgovornosti odnosi na *implementaciju načela zaštite podataka*.[140]

Nalazimo se u epohi, gde je upotreba podataka o ličnosti svakodnevna. Zbog tehnološkog napredka i povećava se količina podataka iz dana u dan. Pojedinci i njihovi podaci prvi su na udaru ovih tehnoloških promena. Sa sve većom upotrebom podataka o ličnosti, koji su dostupni, koji se obrađuju, koji se transferišu, povećava se rizik od zloupotrebe podataka. Sve to ukazuje na upotrebu odgovarajućih delotvornih internih mehanizama, koji bi garantovali zaštitu podataka. Ove obaveze treba da ispune rukovaoci, a kao adekvatan mehanizam preporučuje se uvođenje menadžmenta upravljanja podacima, koji bi umanjio potencijalne pravne, ekonomske i reputacione rizike.

Načelo društvene odgovornosti je bazirano na tome da se zaštita podataka sa nivoa teorijskog i apstraktog razmatranja treba praktično implementirati. Da bi se ovo načelo praktično ostvarilo neophodna je implementacija odgovarajućih mera. Na taj način bi trebalo da dođe do efektivnog ostvarivanja prava na zaštitu podataka. Pored toga ovo načelo instistira na povećanju odgovornosti i jača ulogu rukovaoca.

Stoga ovo načelo obavezuje rukovaoce da preduzmu odgovarajuće i delotvorne mere, kako bi implementirali *načela i obaveze iz OUZP* i kako bi mogli da *na zahtev dokažu adekvatnu implementaciju* (čl. 5 st. 2 OUZP). U praksi to bi značilo implementaciju osnovnih načela zaštite podataka po osnovu compliance - programa.

Pravno gledano načelo društvene odgovornosti se bazira na 2 nivoa. 1. nivo se odnosi na sve obaveze rukovaoca. 2. nivo se odnosi na uvođenje mera odnosno postupaka i odgovarajućih dokaza.

Načelo društvene odgovornosti može biti primenjeno i za obvezujuća korporativna pravila eng. *Binding Corporate Rules* "BRC". Ova pravila se koriste kod multinacionalnih kompanija koje međusobno razmenjuju podatke. BRC sadrže modele ponašanja, interne mere za delotvornu implementaciju načela zaštite podataka. Primena načela društvene odgovornosti može značiti da kompanije pružaju odgovarajući nivo zaštite podataka, te stoga mogu međusobno razmenjivati podatke.

U svrhu ostvarivanja načela društvene odgovornosti služe i mehanizmi *sertifikacije*. Sertifikaciju treba posmatrati kao dokaz, da je rukovalac ispunio načela zaštite podataka i sproveo adekvatne mere, koje je redovno proveravao.[141]

---

[140] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje u vezi sa načelom društvene odgovornosti*, Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht, 00062/10/DE, WP 173 13. 07. 2010, str. 8

[141] *Ibidem*, str. 3, 7, 19.

Rukovalac treba da garantuje *delotvornost mera* i da na zahtev nadzornog organa za zaštitu podataka *dokaže*, da je on zaista implementirao ove mere.

Ovaj zahtev se sastoji iz 2 elementa, koje rukovaoci treba da ispune. Najpre od postavljanja standarda za *implementaciju odgovarajućih i delotvornih mera* da bi došlo do implementacije načela zaštite podataka. Drugi element se sastoji od *dokaza, da su odgovarajuće mere implementirane*.

Koje su to mere koje bi trebalo implementirati, da bi one važile kao odovarajuće. Kao minimalne mere bi mogle biti predviđene one koje bi implementirale načela zaštite podataka uz pomoć internih strategija i procesa. Ove mere bi trebalo da budu predviđene u procesima putem odgovarajuće raspodele poslova i obuke zaposlenih. Kao jedna od mera je i angažovanje ovlašćenog lica za zaštitu podataka.

Primer mera prema mišljenju Radne grupa član 29:

- ✓ Određivanje internog postupka od početka obrade podataka o ličnosti.
- ✓ Uspostavljanje strategije zaštite podataka, koja će uzeti u obzir od početka postupke obrade podataka u skladu sa načelima zaštite podataka.
- ✓ Utvrđivanje postupaka za identifikaciju obrade podataka i vođenje evidencije obrade podataka.
- ✓ Imenovanje ovlašćenog lica za zaštitu podataka.
- ✓ Obuka zaposlenih vezana za zaštitu podataka.
- ✓ Utvrđivanje postupka za obradu zahteva vezanih za prava pojedinaca.
- ✓ Uspostavljanje mogućnosti internih žalbi.
- ✓ Uspostavljanje postupaka za efektivno ophođenje i prijavu bezbedonosnih propusta.
- ✓ Sprovođenje kontole ugovora o zaštiti podataka.
- ✓ Sprovođenje postupka kontrole, koji bi omogućili proveru sprovedenih mera (spoljni i interni audit).

Koje konkretne mere treba sprovesti, trebalo bi odlučiti u zavisnosti od okolnosti obrade podataka i povezanog rizika kao i naravno vrste podataka koji se obrađuju. Koliko je rizik visok, može se odrediti na osnovu obima obrade podataka, svrhe obrade i broja transfera podataka. U tom kontekstu treba uzeti u obzir da li se radi o obradi posebnih kategorija podataka.

Kod kompleksnih, opsežnih obrada podataka, koje su povezani sa visokim rizicima potrebno je redovno *ispitivati delotvornost i proverljivost mera* npr. putem internog ili spoljnog audit-a. Na taj način će biti dokazano i proverljivo da su adekvatne mere implementirane.

Rukovalac ostaje *odgovorno lice i pored implementiranih i kontrolisanih mera*.[142] Sama implementacija mera ne znači da se protiv rukovaoca ne mogu povesti postupci pred nadzornim organom zaštitu podataka. Nadzorni organ zaštitu podataka

[142] *Ibidem*, str.12.

može uzeti u obzir pri odlučivanju o sankcijama sprovođenju ili nesprovođenju mera. Zato se kao dokaz može pružiti ispunjenje adekvatnih mera i načela zaštite podataka.

Zaprećena kazna od 20.000.000 evra ili do 4 % ukupnog svetskog prometa za predhodnu godinu (u zavisnosti koji od ova dva je veći iznos), pokazuje koliko je ostvarivanje načela zaštite podataka bilo značajno zakonodavcu pri određivanju visina kazni.

4.2. Zakonitost obrade podataka

U pravu zaštite podataka postoji posebna maksima „dozvola uz rezervu“, po kojoj je *obrada podataka generalno zabranjena a dopuštena samo uz izuzetke*, kada je to izričito zakonski regulisano ili ako postoji izričit pristanak pogođenih lica (tzv. *zabrana uz dopuštene izuzetke/rezerve*).[143]

Ukoliko se sprovodi obrada podataka o ličnosti bez pristanka pojedinaca ili zakonskog ovlašćenja, obrada je nezakonita. Upravo bazirano na odluci Evropskog suda (po čl. 7 Direktive o zaštiti podataka iz 1995. godine), po sličnosti *dopušteni izuzeci su sadržani u čl. 6 OUZP i države članice EU ne mogu da regulišu dalje dopuštene izuzetke*.

„Da bi obrada bila zakonita, podaci o ličnosti moraju da se obrađuju na osnovu pristanka lica na koje se podaci odnose ili na drugoj legitimnoj osnovi, koja je propisana ili u ovoj uredbi ili u drugom pravu Unije ili pravu države članice..“ (U.t.r. 40 OUZP).[144]

4.2.1. Pristanak (čl. 6 st. 1 a) OUZP)

Pristanak predstavlja samo *jedan od mogućih pravnih osnova za obradu podataka o ličnosti.* U praksi pristanak igra važnu ulogu ne samo za pojedinca nego i za rukovaoca. Punovažan pristanak omogućava pojedincima da steknu *kontrolu vezanu za obradu* njihovih podataka. Stoga je punovažan pristanak od ključnog značaja, da bi se rukovaoci mogli uopšte pozivati na ovaj pravni osnov obrade podataka.

Pristanak se kao pravni pojam koristi i u drugim granama prava, a pre svega u ugovornom pravu. Značajno je da se razgraniči važenje i upotreba pravnih termina, kada se radi o obradi podataka o ličnosti. Norme *ugovornog prava* treba *odvojeno posmatrati* i procenjivati u odnosu na norme prava *zaštite podataka o ličnosti* (npr. punovažnost ugovora – starosna granica, prigovor). Zaštita podataka ne isključuje pristanak po osnovu građanskog prava. To znači da pri proceni važenja jednog

---

[143] Phil Salewski, Alte Grundsätze und neue Rechtmäßigkeitsvoraussetzungen – Teil 3 der Serie zur neuen DSGVO, https:// www. it - recht - kanzlei. de/ alte - grundsaetze-rechtmaessigkeitsvoraussetzungen -neue -datenschutzgrundverordnung. html? print=1, 01.11.2018.

[144] Matthias Schmidl, Leitfaden, Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung, Datenschutzbehörde Republik Österreich, https:// www. dsb. gv. at/ documents/ 22758/116802/ dsgvo -2016 -leitfaden.pdf/ 93d6cb80-8d8e-433d-a492-a827e3ed81a2, 20.07.2017., str. 8.

ugovora kao pravnog osnova obrade (čl. 6 st. 1 b) OUZP) moraju biti procenjene i norme građanskog prava. Identično važi i za procenu punovažnosti pristanka (čl. 6 st.1 a) OUZP).

Generalno za punovažnost pristanaka treba tumačiti definiciju pristanka (čl. 4 tč. 11 OUZP), uslove punovažnosti pristanka (čl. 7 OUZP), i zakonitost pristanka (čl. 6 st.1 a OUZP).

Definicija čl. 4 tč. 11 OUZP

„Pristanak" znači svako dobrovoljno, za svaki konkretan slučaj, na informisan način i nedvosmisleno izražavanje volje pojedinca, kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu podataka o ličnosti koji se na njega odnose.

Važni elementi pristanka su:

- ✓ svako izražavanje volje;
- ✓ dobrovoljnost;
- ✓ za svaki konkretan slučaj;
- ✓ tako da pojedinac bude informisan i nedvosmisleno razume za šta daje pristanak.

Pojam *„svako izražavanje volje"* podrazumeva da se pristanak može izraziti bez ograničenja *u bilo kojoj formi*. OUZP ne reguliše izričito nijednu od formi, ali u uslovima za punovažnost pristanka pojašnjava uslove za punovažnu pisanu formu.

Volja može biti izražena na različite načine, ali je važno da se pritom namere pojedinaca uoče i da one budu jasne za rukovaoca. Stoga izražavanje volje *podrazumeva neophodnu radnju* od strane pojedinaca.Ta radnja može biti pisana (npr. u vidu potpisa), usmena ili u vidu konkludentne radnje iz koje se jasno može zaključiti namera pojedinca.

Veliku nedoumicu predstavlja to, da li odsustvo radnje ili bolje rečeno pasivno ponašanje može biti smatrano kao izraz volje. Sam pojam izraz volje iziskuje ponašanje odnosno radnju. Stoga se može zaključiti da *sam pristanak iziskuje neophodnu radnju*, koju treba procenjivati zavisno od okolnosti. Na pasivnom ponašanju ne može se zasnivati punovažan pristanak.[145]

PRIMER PASIVNO PONAŠANJE
Često u praksi pre svega banke šalju pisma klijentima, u kojima ih informišu o transferu podataka. U takvoj korenspodenciji oni navode da ukoliko klijenti u roku od dve nedelje ne ulože prigovor, da će se smatrati da su pristali na transfer podataka. Na ovakva pisma odgovara u proseku do 10 % klijenata. Ne može se tvrditi da su ostali pristali na transfer podataka. Pošto upravo ne postoji u ovom slučaju jasan izraz volje, rukovalac neće imati adekvatan dokaz pristanka, pa će punovažnost pristanka biti sporna.

[145] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje u vezi definicije pristanka*, Stellungnahme 15/2011 zur Definition von Einwilligung, 01197/11/DE, WP 187, 13.07.2011., str. 13, 14, 15.

PRIMER SLIKE NA PLATFORMI FIRME
Preduzeće se odlučilo da na svojoj internoj platformi postavi ime, prezime, funkciju zaposlenih. Pored toga svaki radnik je zamoljen da pošalje sliku sa svojim imenom, koja bi bila postavljena na platformu. Samo slanje slike radnika se može posmatrati kao pristanak. Takođe i situacija u kojoj preduzeće omogući da svaki od zaposlenih može da ubaci na platformu sliku, što se može posmatrati kao pristanak. Sam čin ubacivanja slika predstavlja radnju, tako da predstavlja pristanak.

Pojam *„dobrovoljnost“* podrazumeva da bi pristanak bio punovažan, mora biti dobrovoljan. To znači da mora biti dat *bez prinude*, ali i da ne sme biti obmane ili negativnih posledica po pojedince, ako ne daju pristanak. Pristanak je punovažan samo onda, kada pojedinac ima *mogućnost izbora*, a ne postoji pritom rizik da će biti obmanut, prinuđen ili imati negativne posledice, ako isti ne da. Svako ograničenje mogućnosti izbora, utiče na to da pristanak ne bude dobrovoljan.

Radna grupa član 29 je tumačila pristanak kod zaposlenih po pitanju toga *šta znači bez prinude*: „Kada se zatraži pristanak zaposlenih i *kada je ne davanje pristanka povezano sa potencijalnim nedostacima po njega*, onda takav pristanak nije punovažan, pošto nije dat dobrovoljno. Kada zaposleni nema mogućnosti da odbije zahtev za obradu podataka, ne može se govoriti o pristanku. Problemi nastaju tamo, gde je pristanak uslov zapošljavanja. Zaposleni ima doduše teoretski pravo da odbije da da pristanak, ali onda mora računati na to da će izgubiti posao. Pod ovakvim okolnostima pristanak nije dobrovoljno dat, te stoga nije punovažan. Još jasnija je situacija kada se svim zaposlenim daju iste predpostavke za zaposlenje“.[146]

PRIMER DOBROVOLJNOST PNR – PODACI
Punovažnost pristanka putnika je sporna, kada se pristanak uzima kao pravni osnov transfera PNR-podataka avio kompanijama u SAD. Pristanak ne može biti u ovom slučaju dobrovoljan, pošto su avio kompanije u obavezi da proslede podatke. Takođe putnici ovom prilikom nemaju pravo izbora. Stoga je jedini mogući pravni osnov transfera podataka izvršenje pravne obaveze u ovom slučaju sporazuma između EU i SAD o transferu podataka putnika (PNR-podataka).

Pojam *„za konkretan slučaj“* predstavlja uslov punovažnosti pristanka. Podrazumeva da pristanak mora biti dat za konkretan slučaj. To znači da paušalni pristanak bez konkretnog određivanja svrhe nije zakonit. Stoga informacije ne smeju biti u „opštim uslovima poslovanja“ kompanije, već je potrebno *odvojiti pristanak od opštih uslova*. Da bi pristanak bio dat za konkretan slučaj to podrazumeva da sam pristanak bude razumljiv. To znači da bude nedvosmislen, da ima određeno područje važenja i da se odnosi na posledice obrade podataka. Kontekst važenja pristanka je stoga ograničen. Pristanak treba da *sadrži navode o podacima koji se obrađuju*, *svrhu*

[146] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje u vezi obradom podataka o ličnosti zaposlenih*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, WP48, 13.09.2001.

obrade podataka. Takođe mora da se bazira na očekivanju pojednica, pošto je ovaj uslov usko vezan sa informisanosti pojedinca.

Sam pristanak mora da sadrži različite elemente, koji se odnose na obradu podataka. Ne sme da se uopšteno odnosi na svrhe i da uopšteno opisuje svrhu, već svrha mora biti proporcionalna i neophodna za konkretnu obradu podataka. Moguće je da *pojedinac da pristanak odjedanput za različite obrade podataka*, ali to mora biti očekivano i proporcionalno za pojedinca.

Pristanak u konkretnom slučaju obavezuje rukovaoca da mora da *informiše pojedince o svakoj promeni svrhe* prvobitne obrade. Tako da pojedinci imaju mogućnost da daju *nov pristanak*.

Radna grupa član 29 je dala mišljenje u pogledu pristanka vezanog za obradu elektronskih akata pacijenata „*Pristanak za konkretan slučaj* mora se odnositi tačno na konkretnu situaciju, u kojoj se dešava obrada medicinskih podataka. Paušalni pristanak pojedinaca npr. putem prikupljanja medicinskih podataka u elektronskim aktima pacijenata i potom transfer medicinskih podataka radi lečenja ostalim stručnim licima, ne bi predstavljao punovažan pristanak".[147]

Pojam *„na način da pojedinac bude informisan"* uključuje primenu čl. 13 i 14 OUZP, kojima se reguliše koje se informacije moraju dostaviti pojedincima. Pored ovih informacija, u kontekstu pristanka se očekuje da rukovalac pruži informacije razumljivim jezikom, tako da pojedincu bude jasno u pogledu koje svrhe je dao saglasnost. Na taj način ovde dolazi do primene zahteva iz čl. 12 OUZP. To podrazumeva da je potrebno izbegavati previše pravne ili tehničke termine. Pored toga informacije moraju biti jasne i upadljive, da ih pojedinac ne bi previdео. Uz to one trebaju biti saopštene direktno pojedincu, a to znači da ne budu "negde" dostupne.

Informisanost pojedinaca je dakle važno obeležje pristanka. Samim tim je *transparentnost preduslov za punovažan pristanak*. Sam pravni osnov obrade na osnovu pristanka je *baziran na informacionom samoodređenju pojedinaca*, tako da ovaj element pristanka treba posmatrati u širem kontekstu. Da bi pristanak bio punovažan, pristanak treba da bude dat „na način da pojedinac bude informisan". To znači i da se pojedincima moraju saopštiti sve relevantne informacije (čl. 13 OUZP) pre davanja pristanka. Takođe ovaj uslov podrazumeva i da najvažniji aspekti obrade podataka moraju biti saopšteni pojedincu. Transparentnost u obradi podataka je jedan od uslova punovažnosti. Stoga se zahteva njeno poštovanje pre početka obrade podataka. Iako sam trenutak davanja pristanka nije regulisan, implicitno se očekuje da se *pristanak pribavi pre početka same obrade podataka*. [148]

---

[147] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Radni papir obrada podataka pacijenata u elektronskim aktima*, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), WP131, 2007.

[148] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje u vezi definicije pristanka,* Stellungnahme 15/2011 zur Definition von Einwilligung, 01197/11/DE, WP 187, 13.07.2011., str. 15, 16, 19. 20, 21, 22, 41.

Uslovi punovažnosti pristanka (čl. 7 OUZP) određuju detaljnije zahteve u pogledu ovog pravnog osnova obrade podataka.

1. Važno je ustanoviti za običan pristanak (za razliku od izričitog) je potrebno dostaviti *dokaz* da se obrada podataka bazira na pristanku.

2. Bitan uslov punovažnosti pristanka kada se radi o *pisanoj formi* je da se sam pristanak *odvoji od ostalih delova ugovora*, opštih uslova poslovanja itd. Sama forma pristanka mora biti sastavljena na jeziku koji pojedinac razume i biti dostupna pojedincima. Osim toga ukoliko ovaj uslov nije u skladu sa OUZP, on nije obavezujući za pojedinca. Zbog toga se može zaključiti da *su ništavne odredbe ugovora, opštih uslova poslovanja koje nisu odvojene od ostalih delova ugovora/opštih uslova poslovanja, koje nisu razumljive lako dostupne pojedincima.*[149]

3. Pristanak je usko povezan sa konceptom informacionog samoodređenja, koji je baziran na autonomiji volje pojedinca. Pristanak je baziran na tome da pojedinac mora biti u poziciji da *dati pristanak opozove*. Sam opoziv se ne odnosi na podatke koji su već bili obrađivani, već ima dejstvo za ubuduće (lat. ex nunc). Sam *opoziv* pristanka mora biti omogućen pojedincima *na jednostavan način*, kao i samo pribavljanje pristanka. O ovom pravu pojedinca mora rukovalac informisati pojedinca *pre* dobijanja pristanka.

4. *Dobrovoljnost* pristanka treba tumačiti procenom situacije vezane za konkretnu obradu. Pitanje je: da li se kao pravni osnov koriste podaci koji su nužni za izvršenje ugovora (uključujući izvršenje usluga ili servisa) ili se radi o pristanku kod kojeg podaci nisu neophodni za izvršenje ugovora. Odgovor na ovo pitanje zavisi od konketne situacije, ali svakako da se načela obrade podataka u ovom kontekstu moraju ispoštovati. To znači da se podaci u skladu sa načelom minimizacije podataka moraju svesti na najmanju moguću meru, koja je neophodna za izvršenje svrhe ugovora.

Kao što je već rečeno, za obradu podataka moguće je da postoji *više pravnih osnova obrade*, koji se mogu primeniti. Treba imati u vidu da kao osnov obrade podataka mora postojati *barem jedan pravni osnov*. Jedan pravni osnov obrade ne isključuje upotrebu više pravnih osnova, ali je važno da se pravni osnovi u pravilnom kontekstu koriste.

Tako je moguće da je određena obrada bazirana na ispunjenju ugovora (čl. 6 st. 1 b) OUZP), a rezultati obrade su neophodni za izvršenje pravne obaveze (čl. 6 st. 1 c) OUZP), dodatne informacije su prikupljene na osnovu pristanka pojedinaca (čl. 6 st. 1 a) OUZP).

PRIMER KUPOVINA AUTOMOBILA
U postupku kupovine automobila rukovalac može koristiti podatke kupca (pojedinca) u različite svrhe i po različitim pravnim osnovama: - Podaci, koji su neophodni za kupovinu automobila (pravni osnov- izvršenje ugovora čl. 6 st. 1 b) OUZP) - Podaci koji služe su neophodni za prijavu vozila (pravni osnov- pravna obaveza čl. 6 st. 1 c) OUZP) - Transfer podataka trećim licima baziran na saglasnosti, radi obavljanja marketinga u sopstvene svrhe (pravni osnov- pristanak čl. 6 st. 1 a) OUZP).

[149] Markus Kastelitz, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 110.

Sam *pristanak* kao pravni osnov *ne oslobađa rukovaoca od obaveza u pogledu pridržavanja načela obrade podataka* (čl. 5 OUZP). Tako pri prikupljanju podataka i pored pristanka pojedinaca, obrada podataka ne bi bila punovažna, ako samo prikupljanje podataka prevazilazi svrhu prikupljanja podataka. Pristanak predstavlja samo jedan pravni osnov i ne oslobađa rukovaoce od primene osnovnih principa zaštite podataka.

Treba imati u vidu da pristanak ne treba da bude prva mogućnost u izboru pravnog osnova obrade podataka. Pre svega iz razloga što pristanak *gubi na vrednosti*, kada se njegova upotreba isuviše proširi ili suzi, da bi se prilagodio određenoj situaciji. Zato je upotreba pristanka u pravilnom kontekstu od suštinskog značaja. Drugim rečima ako se pristanak upotrebljava u situacijiama koje nisu odgovarajuće i gde se to ne očekuje, dovodi se u pitanje punovažnost samog pristanka. U mnogim situacijama kompleksnost pristanka utiče na sposobnost pojedinaca da odluče o korišćenju njihovih informacija. To su pre svega situacije koje se odnose na transparentnost, obimnost i nejasnosću jezika pri pribavljanju pristanka.

Pristanak kao pravni osnov obrade podataka razlikuje se u odnosu na "prezežnije interese" kao pravni osnov (čl. 6 st. 1 f) OUZP). Kada se želi uložiti prigovor po osnovu pristanka, prigovor nije moguće uložiti *pre* početka same obrade podataka. Sa druge strane prigovor po osnovu "pretežnijih interesa"može se uložiti *za vreme* same obrade.[150]

PRIMER IZRIČIT PRISTANAK I PREZEŽNIJI INTERESI
Pošto se za transfer podataka u "treće zemlje" zahteva izričit pristanak, može se reći da je isključena situacija u kojoj bi lice bilo pozvano da da pristanak za transfer podataka, nakon što se on već odigrao.

Pristanak je moguće koristiti uopšteno kao pravni osnov (čl. 6 st. 1 a) OUZP), ali i *u posebnim situacijama*:

- ✓ Pristanak kod obrade podataka dece (čl. 8 OUZP);
- ✓ Izričit pristanak na obradu posebnih kategorija podataka (čl. 9 st. 2 a) OUZP);
- ✓ Izričit pristanak na transfer podataka u "treće zemlje" (čl. 49 st. 1 a) OUZP).

Pristanak kod obrade podataka dece (čl. 8 OUZP) je po prvi put regulisan u pravu zaštite podataka. Koncept dečijeg pristanka odnosi se *samo* na *usluge u onlajn okruženju*. Deca ili bolje rečeno maloletnici su pojam, koji je različito regulisan u državama članicama EU. Stoga je i njihova saglasnost vezana za različite starosne granice.

Važno je da maloletnik, koji *je navršio 16 godina* može *dati punovažan pristanak* bez saglasnosti roditelja za obradu njegovih podataka u onlajn okruženju. „Punoletstvo" u smislu pristanka kao pravnog osnova obrade vezanog za usluge u onlajn okruženju, mogu *države članice EU najviše sniziti do navršenih 13 godina*.

[150] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje u vezi definicije pristanka*, Stellungnahme 15/2011 zur Definition von Einwilligung, 01197/11/DE, WP 187, 13.07.2011., str. 9, 10, 11.

Deca sa *12 i manje godina* moraju dobiti *saglasnost roditelja ili staraoca* vezano za usluge u onlajn okruženju.

Pored toga da bi pristanak bio punovažan, *rukovaoci su obavezi da preduzmu adekvatne tehničke mere kako bi osigurali da roditelj ili staralac da pristanak*. Može se primetiti da je ovaj uslov veoma važan za praksu, pogotovu ako se uzme u obzir korišćenje društvenih mreža (Fejsbuk, Instagram itd.).[151]

Na punovažnost pristanka obrade podataka dece *ne treba primenjivati norme ugovornog prava* kao što su važenje ugovora, sklapanje ugovora i posledice ugovora). To znači da se uslovi punovažnosti pristanka vezanih za decu trebaju gledati samo u smislu OUZP.

Pristanak na obradu posebnih kategorija podataka o ličnosti kao *i* pristanak za *transfer podataka u treće zemlje* mora biti *izričit*. To znači da se očekuje aktivan odgovor usmeni, ili pisani. Ovakav izraz saglasnosti se odnosi na određene svrhe koji se obrađuju. Izraz saglasnosti može biti dat uz pomoć klika na dugme u prozorčiću.

Izričit pristanak se odnosi na sve situacije u kojima osobe mogu dati predlog i u kojima one koriste ili objavljuju svoje podatke bilo sa time da mogu da se *saglase ili* da mogu da *odbiju* obrade podataka. Tom prilikom od značaja je da pojedinci mogu aktivno da odgovore na pitanje pisano. Po pravilu se za izričit pristanak zahteva *pisana forma i potpis* pojedinca.

U onlajn okruženju izričit pristanak može biti dat uz pomoć *digitanog potpisa* ili klikom na ikonice (pozoričiće) / markiranjem polja. Sama upotreba digitalnih potpisa dovodi do visokog nivoa dokaza pristanka.

PRIMER IZRIČIT PRISTANAK
Kada pojedinac formular pristanka potpiše, u kom je objašnjena obrada podataka, postoji jedan izričit pristanak.

Izričit pristanak može se dati i elektronski i usmeno. Sam usmeni pristanak otežava rukovaocu da ga dokaže, pa se može reći da ima manju verodostojnu snagu. Stoga se može reći da sve *varijante opt-out rešenja nisu adekvatne* za punovažnost izričitog pristanka.

PRIMER NEPOSTOJANJE IZRIČITOG PRISTANKA
Kod medicinskih podataka u istraživačke svrhe može postojati situacija, da se pacijent informiše da će njegovi podaci biti transferisani istraživaču, ako on ne uloži prigovor. Ovakav pristanak nije izričit.

Izričit pristanak za slučaj vezan za transfer podataka u „treće zemlje" podrazumeva da se pojedincu predoči konkretan rizik vezan za transfer u treće zemlje, koje nemaju adekvatne mere zaštite, na taj način da se informišu pojedinci (čl. 49 st. 1

[151] Markus Kastelitz, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 111, 112.

OUZP). Identično važi i za *izričit pristanak na obradu posebnih kategorija podataka* (čl. 9 st. 2 a) OUZP).

Za izričit pristanak je važan *kvalitet informacija*. To podrazumeva da način i vrsta informacije moraju biti tako dati (jasno, razumljivo, jednostavnim jezikom), da se objasni konkretan slučaj. Način i vrstu informacije treba odabrati zavisno od okolnosti, ali tako da ih mogu razumeti prosečni korisnici.

Takođe za ovu vrstu pristanka je potrebno da *informacija bude dostupna i vidljiva*. To znači da bude direktno data pojedincu. Informacija ne sme biti negde dostupna, već na način da je pojedinac može pronaći i da je direktno dobio. Pored toga ova informacija mora biti razumljiva, upadljiva i vidljiva (treba obratiti pažnju na veličinu slova).

Radna grupa član 29 je dala mišljenje za upotrebu *pristanka prilikom transfera podataka*. Ustanovljeno je da „pristanak u slučajevima u kojima se ponavlja transfer ili je automatizovan, ne nudi adekvatan pravni osnov obrade podataka rukovaocima na duže staze. Naročito u slučajevima kada transfer podataka nije neophodan, može to za rukovaoce predstavljati nerešive probleme, ako pojedinac naknadno odluči da opozove svoj već dat pristanak. Nakon opoziva ne bi se smeli prosleđivati podaci tog pojedinca. Da bi podaci mogli dalje biti prosleđivani morala bi da postoji alternativa za pojedinca (ugovor, BRC). Stoga pristanak može izgledati kao dobar pravni osnov, koji u praksi može napraviti kompleksne i teško rešive probleme za rukovaoce“.[152] [153]

4.2.2. Izvršenje ugovora (čl. 6 st. 1 b) OUZP)

Izvršavanje ugovora predstavlja takođe jedan od mogućih pravnih osnova obrade podataka, kada je *„obrada neophodna za izvršavanje ugovora u kojem je pojedinac stranka ili kako bi se preduzele radnje na zahtev pojedinca pre sklapanja ugovora”* (čl. 6 st. 1 b) OUZP).

Ovaj zakonski osnov u prvom redu uključuje situacije u kojima je obrada podataka *neophodna* za izvršenje ugovora u kojoj je pojedinac stranka. Stoga ovaj zakonski osnov nije pogodan, ako se žele prikupiti podaci radi pravljenja profila i preferenci kupaca ili klijenata, pošto oni generalno nisu neophodni za izvršenje ugovora.

Neophodnost ili nužnost je i u ovom kontekstu usko povezana sa *načelom ograničenja svrhe obrade podataka*. Stoga treba ispitati da li je u odnosu sadržaj ugovora, cilj ugovora neophodno obrađivati konkretne podatke. To podrazumeva proporcionalnu upotrebu u odnosu na svrhu obrade podataka. Striktno gledano korišćenje tipičnih podataka kao što su ime, prezime, adresa stanovanja, ne bi se smelo po ovom osnovu koristiti u slučaju spora. Ovaj zakonski osnov se odnosi isključivo

[152] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Radni papir o zajedničkom tumačenju čl. 26 st. 1 Direktive 95/46 EZ*, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114, 25.11.2005.

[153] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje u vezi definicije pristanka,* Stellungnahme 15/2011 zur Definition von Einwilligung, 01197/11/DE, WP 187, 13.07.2011., str. 30, 32.

na izvršenje ugovora. Ali bi se podaci mogli upotrebiti za slanje opomena, ukoliko se ugovor ne izvršava. Angažovanje firmi za naplatu potraživanja ne bi spadalo u redovno izvršenje ugovora, pa se stoga ovi podaci po ovom zakonskom osnovu ne bi smeli koristiti. U ovom slučaju bi se pre mogao upotrebiti zakonski osnov „pretežnijih interesa" rukovaoca (čl. 6 st. 1 f) OUZP).

PRIMER
Prikupljanje podataka o adresi stanovanja, kako bi se dostavila određena roba, ako se kupovina vrši putem interneta. Takođe prikupljanje podataka vezanih za plaćanje, da bi se sprovela kupovina robe. U kontekstu zaposlenja bi to bili podaci vezano za račun zaposlenog, kako bi mogla da se isplati zarada.

Ovaj zakonski osnov uključuje obradu podataka koja se odnosi na *predugovorne radnje*, koje su neophodne za izvršenje ugovora. To su situacije kada se potencijalni kupac obrati sa zahtevom za slanje ponude prodavcu neke robe. Tako se ovi podaci mogu čuvati za određeni period i obrađivati shodno zahtevu kao potencijalni kupci. Identično važi i za slanje dokumenata, biografija, svedočanstava u svrhu sklapanja ugovora o radu. Podaci o kandidatima za zaposlenje mogu se čuvati onoliko dugo, koliko je to neophodno radi ispunjenja zakonskih obaveza.[154]

4.2.3. Pravna obaveza (čl. 6 st. 1 c) OUZP)

Pravna obaveza predstavlja jedan od mogućih pravnih osnova obrade podataka, kada je *„obrada neophodna radi izvršenja pravnih obaveza rukovaoca"* (čl. 6 st. 1 c) OUZP).

PRIMER
Kada poslodavac mora da saopšti podake o zaradama zaposlenih zdravstvenom osiguranju ili poreskoj upravi. Takođe može se desiti da su banke ili osiguravajuća društva u obavezi da prijave nadležnoj instituciji moguće pranje novca.

Ovaj zakonski osnov obrade podataka je veoma sličan čl. 6 st. 1 e) OUZP, kada se radi o obradi koja je nužna za izvršavanje zadatka od javnog interesa. Međutim domašaj čl. 6 st. 1 c) OUZP je veoma ograničen, pošto *obaveza obrade podataka mora biti propisana zakonom*. Zakonska regulativa bi morala da uzme u obzir osnovna načela zaštite podataka. Pritom zakonska obaveza treba da bude što je moguće preciznija i jasnija, kako bi se prostor za različito tumačenje sveo na minimum. Pri upotrebi ovog osnova obrade podataka rukovalac ne bi imao pravo izbora, da li će upotrebiti neku drugu zakonsku osnovu, već je u obavezi da istu ispuni. Od značaja je i to da se ti propisi odnose samo

[154] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje 06/2014 o pretežnijim interesima rukovalaca shodno čl. 7 direktive 95/46/EZ*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG vom 9.04.2014., 844/14/EN, WP 217, Str. 21, 22, 23.

na pravo EU ili pravo država članica. Ukoliko se pravna obaveza pripisuje pravo iz neke zemlje van EU, tada EU ili država članica moraju prihvatiti ovu pravnu obavezu u vidu sporazuma ili konvencija.

Države članice EU mogu da preciznije odrede posebne uslove za obradu i druge mere za obezbeđivanje zakonite i pravične obrade po ovom osnovu obrade podataka (čl. 6 st. 2 OUZP).

4.2.4. Vitalni interesi pojedinaca (čl. 6 st. 1 d) OUZP)

Jedan od mogućih pravnih osnova obrade podataka je i situacija, kada je *„obrada neophodna kako bi se zaštitili život i zdravlje pojedinca"* (čl. 6 st. 1 d) OUZP).

Ovaj pravni osnov se razlikuje od osnova obrade osetljivih podataka iz čl. 9 st. 2 c) OUZP, kada se radi o kada se radi o situaciji u kojoj je pojedincu ugrožen život i zdravlje i kada pojedinac nije u stanju iz psihičkih ili fizičkih razloga da da saglasnost.

I ovaj zakonski osnov ima ograničenu primenu, ali treba uočiti bitan element „vitalni interesi pojedinca ili nekog drugog fizičkog lica". Radi se dakle o situacijama života ili smrti.

PRIMER
Kada bi došlo do mogućeg trovanja putnika ili ugrožavanja bezbednosti aviona, moglo bi doći do obrade podataka po ovom osnovu.

Ipak i ovaj osnov obrade podataka treba koristiti restriktivno i tamo gde situacija dopušta pribaviti pristanak pojedinca.[155]

4.2.5. Zadatak od javnog interesa (čl. 6 st. 1 e) OUZP)

Jedan od mogućih pravnih osnova obrade podataka u javnom sektoru je situacija, kada je *„obrada je neophodna za izvršavanje zadatka od javnog interesa ili pri izvršavanju službenih ovlašćenja rukovaoca "* (čl. 6 st. 1 e) OUZP).

Javni interes se odnosi na pravo EU ili države članice EU. Tako da se ova odredba ne odnosi na zemlje van EU. Za razliku od čl. 6 st. 1 c) OUZP ovde ne postoji obaveza da rukovalac mora da obrađuje podatke.

PRIMER
Kada rukovalac sam ima zadatak u javnom interesu ili u vršenju vlasti, kada je obrada neophodna za izvršenje zadatka ili vršenje vlasti. Poreski organi prikupljaju i obrađuju podatke građana iz poreske prijave, da bi mogli da odrede visinu poreza. Advokatska komora, koja vrši javnu vlast, može da pokrene disciplinski postupak protiv svojih članova.

[155] *Ibidem*, str. 24, 25, 26.

Ovaj zakonski osnov obrade se odnosi i na situacije kada rukovalac ne vrši javnu vlast, ali biva zamoljen da prosledi podatke od treće strane, koja obavlja javnu vlast. To može biti slučaj u kojem rukovalac konstatuje da je neko lice izvršilo krivično delo i ovu informaciju prijavi policiji.

Pošto ovaj zakonski osnov obuhvata široki spektar mogućih situacija, koje bi se u praksi primenile, OUZP je predvideo u čl. 21 st. 1 *pravo prigovora pojedinca*. Bazirano na zakonskom osnovu obrade podataka u cilju obavljanja „zadataka u javnom interesu" moguće je obrađivati podatke u svrhu vršenja video nadzora iz razloga bezbednosti, nadzirati e-mail saobraćaj itd. Stoga pravo prigovora predstavlja zakonski balans između prava pojedinaca sa jedne strane i nosioca javne vlasti sa druge strane.[156]

Države članice EU mogu da preciznije odrede posebne uslove za obradu i druge mere za obezbeđivanje zakonite i pravične obrade podataka po ovom osnovu (čl. 6 st. 2 OUZP). Pritom kada se ovaj pravni osnov reguliše na nivou EU ili pravom država članica EU može da sadrži posebne odredbe o: "opštim uslovima kojima se uređuje zakonitost obrade koju vrši rukovalac; vrstama podataka koji se obrađuju; licima na koje se podaci odnose; subjektima kojima podaci o ličnosti mogu da se otkrivaju i svrhe u koje podaci o ličnosti mogu da se otkrivaju; ograničavanju svrhe; rokovima čuvanja; radnjama obrade i postupcima obrade, uključujući i mere za obezbeđivanje zakonite i pravične obrade, kao što su mere za druge posebne situacije obrade iz Poglavlja IX" (čl. 6 st. 3 OUZP). Od presudnog značaja je *podaci o ličnosti koji budu obrađivani u svrhe javnog interesa budu neophodni za ostvarivanje te svrhe* "pravom EU ili pravom države članice mora da se ostvari cilj od javnog interesa i mora da bude srazmerno zakonitom cilju kojem se teži" (čl. 6 st. 3 OUZP).

4.2.6. Pretežniji interesi (čl. 6 st. 1 f) OUZP)

Jedan od mogućih pravnih osnova obrade podataka je „pretežniji (*legitimni*) interes". Zbog njegovog učestalog korišćenja u praksi, biće mu posvećena detaljnija pažnja i objašnjenje. Ovaj osnov se odnosi na situaciju, kada je „obrada neophodna za potrebe legitimnih interesa rukovaoca ili treće strane, ukoliko ti interesi nisu pretežniji u odnosu na interese osnovnih prava i sloboda pojedinaca, koji zahtevaju zaštitu podataka o ličnosti, naročito ako je pojedinac dete. Tačka (f) prvog stava ne odnosi se na obradu koju sprovode tela javne vlasti pri izvršavanju svojih zadataka" (čl. 6 st. 1 f) OUZP).

Pojam „*interesi*" stoji neposredno u vezi sa svrhom obrade podataka. Dok sa jedne strane svrha obrade podataka predstavlja razlog, nameru obrade, interesi sa druge strane se odnose na *korist* koju rukovalac može izvući iz obrade podataka. Sam karakter interesa može biti različit od opštih interesa javnosti kao što je npr. sprečavanje korupcije, sloboda štampe, protoka informacija, naučna istraživanja, pa sve do privatnih, ekonomskih itd.

---

[156] *Ibidem*, str. 27, 28, 29.

Sta su "opravdani", a šta "neopravdani" (legitimni ili nelegitimni) interesi, odnosno čiji su interesi pretežniji, predpostavlja *procenu između dve strane*. Najčešće situacije u praksi se odnose na sukobe interesa u sledećim oblastima:

- ✓ Pravo na slobodu izražavanja i informisanja, uključujući medije i umetnost,
- ✓ Direktan marketing i drugi oblici marketinga ili oglašavanja,
- ✓ Sprovođenje pravnih zahteva u vanparničnom postupku,
- ✓ Sprečavanje prevare, zloupotreba vlasti ili pranje novca,
- ✓ Nadzor radnika zbog bezbednosti ili administrativnih razloga,
- ✓ Propisi o prijavljivanju masovnih zloupotreba,
- ✓ Lična bezbednost, IT i bezbednost mreže,
- ✓ Obrada u istorijske, naučne ili statističke svrhe.

Da bi se interesi mogli smatrati opravdanim, potrebno je da rukovalac interese usaglasi sa pravom zaštite podataka i ostalim eventualno primenljivim pravima. Bolje rečeno *opravdani interesi moraju biti pravno dopušteni*. Suština je da sam opravdani interes nije dovoljan element da bi se moglo pozivati na ovaj osnov obrade podataka.

PRIMER
Rukovalac može imati opravdani interes da otkrije navike svojih klijenata, da bi mogao bolju u precizniju ponudu roba ili usluga da im pošalje. Tom prilikom potrebno je da uzme u obzir i određene zaštitne mere, kao što je u ovom slučaju pravo prigovora klijenta. To ne znači da bi samo pravo prigovora bilo dovoljno da opravda interes rukovaoca, ukoliko bi klijenti bili konstantno praćeni u onlajn okruženju bez njihovog znanja, a pritom korićena ogromna količina podataka, izrađivani njihovi profili itd. Samo profilisanje predstavlja značajano zadiranje u privatnost klijenata, pa se može reći da njihovi interesi pretežu u odnosu na interese rukovalaca.

Kada se kod rukovaoca *ne radi o neophodnim interesima*, verovatnije je da će biti opravdaniji interesi pojedinaca. To su situacije kada su interesi rukovaoca manjeg značaja od interesa pojedinaca.

Kriterijum neophodnosti je usko vezan sa načelom vezanosti za svrhu obrade podataka. Tako obrada podataka *mora biti neophodna u svrhu opravdanih interesa*, koja se tiče rukovalaca ili trećih lica. Na taj način dolazimo do toga da je neophodnost prilikom obrade podataka usko vezana i za interese. Stoga je na ovom mestu potrebno takođe proceniti, da li se ista svrha (cilj) može postići sa drugačijim merama, koji bi manje zadirali u prava pojedinaca.[157]

Opravdani interesi u javnom sektoru su isključeni iz primene ovog osnova obrade podataka. To naravno ne znači da za javni sektor nije predviđena zakonska

[157] Radna grupa član 29, Artikel 29 Datenschutzgruppe, *Mišljenje 06/2014 o pretežnijim interesima rukovalaca shodno čl. 7 direktive 95/46/EZ*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG vom 9. April 2014, 844/14/EN, WP 217, Str. 30, 31, 32, 33, 37.

obrada podataka. Ona predstavlja poseban pravni osnov obrade podataka, koji je regulisan čl. 6 st. 1 e) OUZP.

Opravdan interes trećih lica predstavlja čestu situaciju u praksi.

PRIMER
Objavljivanje podataka u svrhu transparentnosti i u okviru društvene odgovornosti. To bi bila situacija, kada bi se objavljivali podaci rukovodećih struktura u nekoj firmi.

Ovakve situacije ne služe dakle interesima rukovaoca, već više *interesima drugih interesnih grupa* kao što su npr. zaposleni, šira javnost.

Radi osiguranja pravne sigurnosti potrebno je u ovom kontekstu potražiti postoji li zakonski osnov za objavljivanje podataka i svrhe transparentnosti ili društvene odgovornosti. Ukoliko postoji, tada bi došlo do primene drugog osnova obrade podataka shodno čl. 6 st. 1 c) OUZP. Ukoliko ne postoji ovaj zakonski osnov i tada bi se mogao primeniti zakonski osnov "pretežnijih opravdanih interesa treće strane". Preduslov za to je procena posledica po pojedince i implementacija odgovarajućih tehničko-organizacionih mera zaštite.

Interesi u pogledu osnovnih prava i sloboda pojedinaca prema mišljenju Radne grupe čl. 29 nisu ograničeni samo na osnovna (temeljna) prava i slobode pojedinaca. Zaštita pojedinaca odnosi se na neophodnost procene svih relevantnih interesa pojedinaca.[158]

Osnovna prava pojedinaca vrlo često mogu biti međusobno suprotstavljena i stajati u suprotnosti sa pravom zaštite podataka. Tako imamo sukob osnovnog prava na zaštitu podataka sa:

- ✓ pravom na slobodu informisanja/mišljenja,
- ✓ pravom svojine,
- ✓ pravom na slobodu i sigurnost,
- ✓ pravom delotvornog pravnog leka,
- ✓ pravom na predpostavku nevinosti.

Pravni osnov obrade podataka „pretežniji interesi" kao što je već spomenuto zahteva *prednodnu procenu proporcionalnosti interesa* od strane rukovaoca.

Za razliku od pristanka kao osnove obrade podataka, koja ne zahteva procenu, sve ostale osnove obrade podataka zahtevaju predhodnu procenu primenljivosti. Samo dakle pristanak kao zakonski osnov obrade podataka ne zahteva predhodnu procenu.

Procena proporcionalnosti interesa se ne svodi na samo procenu interesa dve strane (ili čak i tri strane), već predpostavlja uzimanje u obzir mnogobrojnih faktora. Na taj način je jedino moguće pouzdati se u ovaj zakonski osnov obrade podataka, kao i da su uzeti svi faktori u obzir.

[158] *Ibidem*, str. 33, 34.

Faktori koji treba uzeti u obzir pri proceni su:

- ✓ Vrsta i izvor pretežnijih (opravdanih) interesa,
- ✓ Procena uticaja u vezi sa zaštitom podataka,
- ✓ Dodatne garancije odnosno mere zaštite (transparentnost, smanjenje količine podataka, upotreba adekvatnih tehonologija itd.).[159]

Rezultat ove procene interesa treba da pokaže da li se čl. 6 st. 1 f) OUZP *može uzeti kao zakonska osnova za obradu podataka*. Moze se reci da pozivanje na pretežnije interese *zahteva predhodnu procenu posledica po pojedince*. Stoga bi korišćenje ove mogućnosti obrade podataka uvek uslovljavalo primenu čl. 35 OUZP.

Procena pretežnijih interesa treba da obuhvati i *osnovna načela zaštite podataka* (čl. 5 OUZP). U slučaju da postoji pretežniji opravdan interes u nekom slučaju za obradu podataka od strane rukovaoca, to nikako ne znači da bi rukovalac mogao po slobodnoj volji da prikuplja i obrađuje podatake, koje prevazilaze svrhu obrade podataka. To bi bilo u suprotnosti sa načelom vezanosti za svrhu obrade podataka.

Test procene proporcionalnosti interesa je neophodno sprovesti kako bi se utvrdile posledice po pojedince. Sve dok su opravdani interesi rukovaoca *neznatni* i *nisu neophodni*, može se uopšteno reći da prednost imaju interesi pojedinaca, ako su posledice po ove interese neznatne.

Sa druge strane mogu se opravdati važni i opravdani interesi u određenim situacijama, ukoliko i dođe do masovnog zadiranja u prava pojedinaca ili značajnih posledica po pojedince, ako je rukovalac preduzeo odgovarajuće *tehničko-orgnizacione mere*. Ove mere utiču na umanjenje rizika po posledice pojedinaca, te na taj način utiču na to da se pretežniji interesi pomere u korist rukovaoca. Sama upotreba mera zaštite nije dovoljna da bi se opravdala svaka situacija obrade podataka. Te se stoga savetuje da se procene i ostali kriterijumi.

Procena uticaja u vezi sa zaštitom podataka treba da obuhvati puno elemenata, kako bi se došlo do adekvatnog rezultata. Neki od elemenata su:

- ✓ posledice po pojedince i težina tih posledica, kao i verovatnoća i konsekvence ukoliko nastupe (procena rizika);
- ✓ vrsta i način obrade podataka o ličnosti;
- ✓ očekivanja pogođenih pojedinaca;
- ✓ mišljenje pogođenih pojedinaca;
- ✓ upotreba mera zaštite.

Posto procena uticaja u vezi sa zaštitom podataka nije ništa drugo nego ukupna *procena rizika* po konkretnu obradu podataka, neophodno je proceniti posledice tj. *konsekvence* po pojedinca. To mogu biti iritacija, strah, ljutnja, ako pojedinci izgube

[159] *Ibidem*, str. 3, 4, 6, 11.

kontrolu nad svojim podacima. Takođe to može biti i u situacijama kada bi pojedincima bio narušen ugled ili njihovi podaci zloupotrebljeni.

Procena verovatnoće, da dođe do posledica je bitan element procene rizika po pojedince. Npr: razmena podataka koji izlaze izvan EU, pristup internetu, korišćenje nebezbednih kanala komunikacije (mejlova za transfer osetljivih podataka). Uopšte izvori opasnosti utiču na procenu visine verovatnoće, da bi određena posledica nastupila.

Procena uticaja u vezi sa zaštitom podataka treba da obuhvati i procenu *težine posledica po pojedince*. Kao kriterijum bi se mogao uzeti broj potencijalno pogođenih osoba.

Vrsta podataka je bitna pri proceni, da bi se ustanovilo da li se radi o osetljivim podacima o ličnosti.

Radna grupa čl. 29 smatra da upotreba biomerijskih podataka u svrhe bezbednosti imovine ili ljudi predstavlja opravdani interes nasuprot kome stoji pretežniji interes pogođenih lica. Sa druge strane mogu biometrijski podaci poput otiska prstiju, prepoznavanja lica povećati nivo bezbednosti u osetljivim područjima laboratorija, tako da u tom slučaju mogu biti pretežniji interesi na strani rukovaoca. Za to je neophodno da rukovalac poseduje odgovarajuće dokaze, da visok rizik postoji, ukoliko bi došlo do mogućnosti širenja zaraza i uopšte opasnosti po zdravlje ljudi. Generalno treba imati u vidu da što su osetljiviji podaci o ličnosti, to su teže posledice moguće po pojedince.

Tom prilikom treba videti i o kojoj *kategoriji pojedinaca* se radi. Da li su u pitanju deca, psihičko obolele osobe, radnici, pacijenti. Ukoliko se radi o ugroženim kategorijama pojedinaca, svakako da treba obratiti posebnu pažnju ukoliko se radi o posebno osetljivim kategorijama pojedinaca (deca, osobe sa invaliditetom..) radi primene afirmativnih mera kako bi se oni zaštitili od zloupotrebe podataka kojoj mogu biti izloženi.

Način obrade i to kako se podaci obrađuju služi tome da se proceni, da li su podaci objavljeni i dostupni velikom broju ljudi, koja se količina podataka obrađuje ili kombinuje sa drugim podacima. Tako je moguće da naizgled obični podaci, ukoliko se radi o velikoj količini podataka o ličnosti, mogu u kombinaciji da dovedu do preciznih zaključaka o nekoj osobi i otkriju najintimnije sfere pojedinca. Treba imati u vidu da takve analize mogu dovesti do pogrešnih zaključaka i prognoza, pogotovu ako se radi o ponašanju ili ličnosti pogođenog lica.

Očekivanja pogođenih pojedinaca se odnosi na procenu situacije, da li su pogođena lica mogla da očekuju tu obradu podataka. To bi bila situacija objavljivanja podataka u kojoj bi trebalo proceniti odnos između rukovaoca i pogođenih. Tom prilikom bi trebalo uzeti u obzir, poziciju rukovaoca u odnosu na pojedinca, vrstu i odnos pružanja servisa ili usluga, pravne ili ugovorne obaveze. Generalno važi da što je specifičniji i restriktivniji kontekst prikupljanja podataka, to je za očekivati da će uopšteno veća verovatnoća biti da korišćenje podataka bude ograničeno.

Mišljenje pogođenih pojedinaca je takođe od značaja za celokupnu procenu rizika. Ova mogućnost daje pojedincima šansu da ukažu na opasnosti po zaštitu njihovih podataka, a ujedno je i pokazatelj raspoloženja pojedinaca o nameravanoj

obradi podataka. Podložna je vrednosnim sudovima pojedinaca.[160]

Upotreba mera zaštite može dovesti da umanjenja rizika po posledice za pojedince.

Mere zaštite mogu biti:

- ✓ tehničke i organizacione mere: pseudonimizacija, enkripcija,
- ✓ uvođenje koncepta privacy by design,
- ✓ transparentnost,
- ✓ pravo prigovora,
- ✓ pravo prenosivosti podataka.

Za *enkripciju i pseudonimizaciju* generalno važi pravilo da upotrebom ovih mera zaštite pri proceni uticaja u vezi sa zaštitom podataka i ukupnoj proceni opravdanih interesa, *interesi prezežu na strani rukovaoca ako se koriste ove tehnike*. Sama upotreba ovih tehnika smanjuje verovatnoću za nastupanje posledica po pojedince.

Treba imati u vidu da samo korišćenje enkripcije ili pseudonimizacije ne dovodi do toga da nezakonita obrada podataka može biti proglašena zakonitom, već da ove tehnike utiču pre svega na smanjenje rizika.

Načelo transparentnosti zahteva od rukovaoca da objasni pogođenim licima konkretnu situaciju obrade i zbog čega njegovi interesi pretežu. Pored toga rukovalac treba da ukaže na pravo prigovora pojedincima, kao i na preduzete mere zaštite. Za ovo načelo je od značaja i utiče u kontekstu opravdanja korišćenja pravnog osnova obrade podataka, da li je rukovalac obavestio pojedince o obradi na transparentan način. Svakako da bi sitna slova nekog ugovora bila u suprotnosti sa ovim načelom i u suprotnostima sa očekivanjima pojedinaca.

Načelo društvene odgovornosti zahteva od rukovaoca da najpre proceni interese, ukoliko želi da koristi ovaj zakonski osnov obrade podataka. Razultate ovog testa treba dokumentovati, radi uvida od strane pogođenih pojedinaca, Institucija za zaštitu podataka i svih ostalih zainteresovanih strana.

Pravo prigovora **(**čl. 21 st. 1 OUZP): "pojedinac ima pravo da iz razloga svoje posebne situacije u svakom trenutku uloži prigovor na obradu podataka o ličnosti koji se odnose na njega, u skladu sa članom 6. stav 1. tačka e) ili f), uključujući izradu profila koja se bazira na tim odredbama. Rukovalac više ne sme da obrađuje podatke o ličnosti, osim ako dokaže da postoje neophodni legitimni razlozi za obradu koji prevazilaze interese, prava i slobode pojedinaca ili radi postavljanja, ostvarivanja ili odbrane pravnih zahteva".

Upravo je čl. 6 st. 1 f) OUZP pogođen pravom prigovora pojedinca, koji *ukoliko bude uložen zahteva dodatnu procenu situacije*. Ta procena situacije se odnosi na to da li će se obrada podataka nastaviti ili će podaci biti obrisani. Ukoliko rukovalac ima i dalje pretežniji interes u odnosu na pojedince, on može nastaviti sa obradom podataka

[160] *Ibidem*, str. 39, 47, 48, 49, 50, 51, 52.

ili ukoliko je dalja obrada podataka neophodna radi ispunjenja pravnih zahteva (npr. obaveza čuvanja podataka shodno zakonu).

Izuzetak od ovog pravila tiče se situacije kada pojedinac uloži prigovor po osnovu direktnog marketinga (čl. 21 st. 2 OUZP). Tada ne postoji opravdanje i izuzetak te rukovalac mora obrisati podatake. Stoga se u tim slučajevima predpostavlja opravdan interes pojedinca, da ovakve obrade spreči.[161]

Prenosivost podataka može igrati ulogu u proceni opravdanih interesa, na način što će se kontrola podataka omogućiti pojedincima. Ova mogućnost je naročito od značaja u onlajn okruženju, što može doprineti tome da se pozicija pojedinca ojača. Sama dostupnost mehanizama kontrole podataka od strane pojedinaca omogućava im da steknu ujednačenu poziciju u odnosu na rukovaoca.

Uloga „opravdanih interesa" kao zakonskog osnova obrade podataka sastoji se u adekvatnoj primeni. I ovaj zakonski osnov obrade podataka je jednakog ranga kao i svi ostali iz čl. 6 OUZP. Stoga se ne može reći da ga treba koristiti kao poslednju mogućnost ili kao zamenu za ostale pravne osnove. Sama upotreba u pravilnom kontekstu je od ključnog značaja uz adekvatnu primenu zaštitnih mera, a sami "opravdani interesi" često mogu biti upotrebljeni umesto "pristanka" ili "neophodnosti za izvršenje ugovora" kao pravnih osnova obrade podataka.

Kontrolna pitanja čl. 6 st. 1 f) OUZP
✓ korak: procena situacije, koji pravni osnov obrade bi se mogao primeniti shodno čl. 6 st. 1 a-f OUZP
✓ korak: procena interesa „legitimnih" ili „nelegitimnih"
✓ korak: procena da li je obrada neophodna za ostvarivanje interesa
✓ korak: procena između prava pojedinaca i ostalih prava (pravo na informisanje, pravo svojine itd.)
✓ korak: procena uticaja u vezi sa zaštitom podataka
✓ korak: procena mera zaštite
✓ korak: procena po uloženom pravu prigovora pojedinca
✓ korak: dokumentovanje

4.2.7. Obrada u drugu svrhu u odnosu na prvobitnu (čl. 6 st. 4 OUZP)

Još jedan od elemenata dopuštenosti obrade podataka odnosi se na situacije tzv. *dalje obrade podataka*. To su situacije kada rukovalac ima nameru da podatke koristi u druge svrhe u odnosu na prvobitno prikupljenu svrhu. Iako je ovaj uslov dopuštenosti u suprotnosti sa načelom vezanosti za svrhu obrade (čl. 5 st. 1 c) OUZP) i sa čl. 8 st. 2 Povelje EU o osnovnim pravima, uredba dopušta rukovaocima da uzmu kao validan pravni osnov tzv. „*test usklađenosti/kompatibilnosti svrha*" (prvobitne i nove).

[161] *Ibidem*, str. 53, 54, 55, 56, 57.

Kriterijumi koje tom prilikom treba rukovaoci da uzmu su sledeći:

- ✓ svaka veza između svrha u koje su podaci o ličnosti prikupljeni i svrha nameravane dalje obrade,
- ✓ kontekst u kojem su podaci o ličnosti prikupljeni, posebno u pogledu odnosa između lica na koje se podaci odnose i rukovaoca,
- ✓ priroda podataka o ličnosti, posebno činjenica da li se obrađuju posebne kategorije podataka o ličnosti u skladu sa članom 9 ili podaci o ličnosti koji se odnose na krivične osude i krivična dela u skladu sa članom 10,
- ✓ moguće posledice nameravane dalje obrade za lica na koje se podaci odnose,
- ✓ postojanje odgovarajućih mera zaštite, koje mogu da obuhvataju enkripciju ili pseudonimizaciju.

Potrebno je pre svega ispitati da li je pri nameravanoj daljoj obradi podataka bitno promenjen položaj pojedinaca (pogođenih lica) u odnosu na rukovaoca. To se može odnositi na situaciju u kojoj se pri daljoj obradi podataka u značajnoj meri prikupljaju dodatni podaci o ličnosti. Pri daljoj obradi pseudonimizovanih podataka u cilju dobijanja novih podataka bi test usklađenosti bio ispunjen, ukoliko rezultat dalje obrade podataka ne bi vodio ka određenoj osobi.[162]

U slučaju da test pokaže *usklađenost prvobitne sa novom svrhom, nije potrebno tražiti novi pravni osnov obrade*, pošto se smatra da je obrada podataka već dopuštena (U.t.r. 50 OUZP). To bi značilo da rukovaoci koji već pri prikupljanju podataka znaju i svesni su da će dolaziti do dalje obrade podataka u odnosu na probitne svrhe, treba da uzmu u obzir navedene kriterijume (pre svega se to odnosi na upotrebu BIG DATA alata). Međutim, s obzirom na to da do sada u praksi nije pokazana jasna primena ovih kriterijuma, koja bi garanovala pravnu sigurnost za rukovaoce, *da pored ovog kriterijuma bude obezbeđen i neki od drugih pravnih osnova* iz čl. 6 st. 1 OUZP. Osim toga *savetuje se i sprovođenje procene uticaja u vezi sa zaštitom podataka* (čl. 35 OUZP).

Ukoliko rezultat ovog testa bude u neusklađenosti nove obrade podataka sa prvobitnom obradom podataka, tada je potrebno proceniti da li su ispunjeni uslovi za zakonitu dalju obradu podataka (čl. 6 st. 4 OUZP):

- ✓ pristanak pojedinca za dalju obradu podataka,
- ✓ posebno zakonsko odobrenje shodno propisima EU ili država članica, kojime je izričito regulisana dalja obrada podataka shodno čl. 23 st. 1 OUZP.

Posebno odobrenje dalje obrade podataka shodno čl. 23 st. 1 OUZP, kada se radi o ograničenju načela vezanog za svrhu obrade podataka, mora da „*garantuje suštinu osnovnih ljudskih prava i sloboda* i da predstavlja *nužnu i srazmernu meru* u demokratskom društvu“ u pogledu navedenih ciljeva.

[162] Waltraut Kotschy, *Zweckbindungsprinzip und zulässige Weiterverarbeitung*, Debattenbeitrag zur Datenschutz-Grundverordnung, 23.06.2016., str. 6 fusnota 11.

Ti ciljevi mogu biti:

- ✓ nacionalna bezbednost,
- ✓ odbrana,
- ✓ javna bezbednost,
- ✓ sprečavanje, istraga, otkrivanje ili progon krivičnih dela ili izvršavanje krivičnih sankcija (uključujući zaštitu od pretnji javnoj bezbednosti i njeno sprečavanje),
- ✓ drugi važni ciljevi od opšteg javnog interesa EU ili države članice (naročito važnog privrednog ili finansijskog interesa EU ili države članice, što uključuje monetarna, budžetska i poreska pitanja, javno zdravlje i socijalnu zaštitu),
- ✓ zaštita nezavisnosti pravosuđa i sudskih postupaka,
- ✓ sprečavanje, istraživanje, otkrivanje i progon kršenja etike za regulisane struke,
- ✓ funkcije praćenja, inspekcije ili regulatorne funkcije koja je, barem povremeno, povezana sa izvršavanjem javne vlasti (u slučajevima iz čl. 23 st. 1 a - e i slovo g),
- ✓ zaštita pojedinaca ili prava i sloboda drugih,
- ✓ ostvarivanja potraživanja u građanskim sporovima.

S obzirom na širok spektar ograničenja načela vezanosti za svrhu zaštite podataka pre svega u javnom interesu, može se zaključiti da je *opravdanje dalje obrade podataka uz pristanak pojedinaca dopušteno samo u privatnom sektoru.*

Kao primer nepostojanja neusklađenosti (bolje rečeno usklađenosti!!) prvobitne obrade podataka sa novom obradom podataka čl. 5 st. 1 b) OUZP navodi obradu podataka u svrhe naučnog istraživanja i u svrhe arhiviranja u javnom interesu (U.t.r. 50 OUZP).[163] Ovaj primer dalje obrade podataka naveden u samoj uredbi kao *dodatni element procenjivanja dopuštenosti odnosno zakonitosti obrade podataka* u navedene svrhe.[164]

Zbog čega je zakonodavac svrhe naučnog istraživanja i svrhe arhiviranja u javnom interesu naveo kao primer gde postoji usklađenost prvobitne i nove svrhe obrade podataka (u engleskom prevodu glasi „gde se svrhe ne smatraju nekompatibilnim/neusklađenim"), ostaje nejasno. I pored privilegije iz čl. 5 st. 1 b) OUZP *potrebno je uraditi test usklađenosti u kontekstu načela vezanosti za svrhu obrade podataka.*

Uzimajući sve u obzir može se zaključiti da je *dalja obrada podataka dopuštena u sledećim situacijama*:

- ✓ pristanak pojedinca za dalju obradu podataka, ili
- ✓ posebno zakonsko odobrenje shodno propisima EU ili država članica, kojime je izričito regulisana dalja obrada podataka shodno čl. 23 st. 1 OUZP, ili

[163] U.t.r. 50 OUZP razjašnjava i pokazuje nameru zakonodavca regulisanjem privilegije iz čl. 5 st. 1 b) OUZP. Shodno toj privilegiji se dalja obrada podataka u svrhe naučnog istraživanja i u svrhe arhiviranja u javnom interesu smatra dopuštenom i usklađenom sa prvobitnom svrhom obrade podataka.

[164] Waltraut Kotschy, *Zweckbindungsprinzip und zulässige Weiterverarbeitung*, Debattenbeitrag zur Datenschutz-Grundverordnung, 23.06.2016., str. 4.

- ✓ obrade podataka u svrhe naučnog istraživanja i u svrhe arhiviranja u javnom interesu (čl. 89 u vezi sa čl. 5 st. 1 b) OUZP), ili
- ✓ pozitivan rezultat testa usklađenosti/kompatibilnosti (čl. 6 st. 4 OUZP).[165]

4.3. Zakonitost obrade posebnih kategorija podataka (čl. 9 OUZP)

Dopuštenost obrade posebnih kategorija podataka tzv. *osetljivih podatka* je takođe regulisana u OUZP.

U osetljive kategorije podataka (čl. 9 st. 1 OUZP) spadaju:

- ✓ Podaci o rasnom i etničkom poreklu,
- ✓ Podaci o političkom opredeljenju,
- ✓ Podaci o verskim ili filozofskim ubeđenjima,
- ✓ Podaci o članstvu u sindikatima,
- ✓ Zdravstveni podaci,
- ✓ Podaci o seksualnom životu ili seksualnoj orijentaciji,
- ✓ Genetički podaci,
- ✓ Biometrijski podaci.

Za osetljive podatke je zabrana obrade izričito formulisana, uz takođe dozvoljene izuzetke.

Navedeni osetljivi podaci smeju se obrađivati isključivo u sledećim slučajevima (čl. 9 st. 2 OUZP):

- ✓ Na osnovu *izričitog pristanka pojedinaca*;
- ✓ Ako je *obrada neophodna radi izvršavanja dužnostii posebnih prava* rukovaoca ili lica na koje se podaci odnose *u oblasti prava zapošljavanja i prava socijalnog osiguranja i socijalne zaštite*, ako to dozvoljava pravo Unije ili države članice ili kolektivni ugovor u skladu sa pravom države članice koje propisuje odgovarajuće zaštitne mere za osnovna prava i interese lica na koje se podaci odnose;

Ovaj zahtev se odnosi na radnopravne odnose *i dopunjuje zahtev dopuštenosti „pravna obaveza" iz čl. 6 st. 1 c) OUZP. Tako je primera radi postoji zakonska obaveza prijavljivanja povreda na radu, bolovanja radi ostvarivanja prava na zaradu, socijalnu pomoć.*

- ✓ *Ako je obrada neophodna radi zaštite života i zdravlja pojedinaca, ili* kada lice na koje se podaci odnose fizički ili pravno nije sposobno da dâ pristanak;

[165] Markus Kastelitz, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 102, 103.

Radi se o situaciji u kojoj je pojedincu ugrožen život i zdravlje. *Ovaj zahtev dopuštenost obrade je kompatibilan onom iz čl. 6 st. 1 d) OUZP, s tim što u ovom slučaju je neophodno da pored ugroženosti života i zdravlja lica ono* ili fizički nije u stanju ili nije pravno sposobno da pristanak. *To bi mogle biti situacije gde je neko lice povređeno u saobraćajnoj nesreći i da fizički nije u stanju da da pristanak. Takođe situacija u kojoj je nekom licu zbog duševne bolesti oduzeta poslovna sposobnost, a pritom je neophodna obrada njegovih podataka u svrhu lečenja.*

- ✓ Ako se obrada sprovodi u okviru svojih legitimnih aktivnosti, uz odgovarajuće garancije, koju vrši *fondacija, udruženje ili bilo koje drugo neprofitno telo s političkim, filozofskim, verskim ili sindikalnim ciljem*, i to pod uslovom da se obrada odnosi isključivo na članove tog tela ili na lica koja imaju redovne kontakte s njim u vezi s njegovom svrhom i da se podaci o ličnosti ne otkrivaju izvan tog tela bez pristanka lica na koja se podaci odnose;

Ovaj zahtev dopuštenosti obrade osetljivih podataka je određen na podatke o političkim opredeljenjima, članstvu u sindikatima, filozofskim ili verskim ubeđenjima.

Navedene kategorije osetljivih podataka predstavljaju prvi kriterijum *vezan za dopuštenost obrade po ovom osnovu.*

Drugi kriterijum *po ovom osnovu obrade je dat alternativno. Neophodno da se obrada navedenih kategorija podataka vrši isključivo za* članove fondacije ili udruženja ili neprofitnog tela ili da postoje redovni kontakti *sa fondacijom ili udruženjem ili neprofitnog tela.*

Treći kriterijum *je da se podaci koji se obrađuju na ovaj način* ne smeju otkrivati bez pristanka lica izvan tela *(fondacije, udruženja, neprofitnog tela)*.

- ✓ Ako se obrada odnosi na podatke o ličnosti, koje su *pojedinci očigledno sami objavili*;

Ovaj kriterijum dopuštenosti obrade osetljivih podataka o ličnosti je izuzetno problematičan i otvara mogućnost manipulacije i pravne nesigurnosti u praksi. To bi značilo da su podaci o ličnosti koji su očigledno sami objavljeni od strane pojedinaca dopušteni za dalju obradu od strane bilo kojih rukovaoca. Tako primera radi skeniranje lica i fotografiju lica (kao biometrijske podatke) preuzetu sa Fejsbuka mogu obrađivati druge firme ili državne institucije u sopstvene svrhe, jer je fotografija i uz obeležavanje lica očigledno objavljeno od samih korisnika Fejsbuka. Svakako da ovaj kriterijum ne potiskuje ostale uslove dopuštenosti obrade podataka iz čl. 6 st. 1 OUZP.

- ✓ *Ako je obrada neophodna za uspostavljanje, ostvarivanje ili odbranu pravnih zahteva ili za postupanje sudova* u pravosudnim aktivnostima;

Ovaj uslov dopuštenosti je primenljiv na obrade podataka u sudskim postupcima.

- ✓ *Ako je obrada neophodna za potrebe značajnog javnog interesa*, na osnovu

prava Unije ili prava države članice koje je srazmerno željenom cilju i kojim se poštuje suština prava na zaštitu podataka i obezbeđuju primerene i posebne mere za zaštitu osnovnih prava i interesa lica na koje se podaci odnose;

Obrada za potrebe značajnog javnog interesa predstavlja dopunu čl. 6 st. 1 d) OUZP. Ovaj pravni standard ostavlja širok prostor za tumačenje u praksi.

Prvi kriterijum je dakle *značajan javni interes*.
Drugi kriterijum je *poštovanje suštine prava zaštite podataka* (poštovanja načela zaštite podataka iz čl. 5 OUZP).
Treći kriterijum je *primena adekvatnih mera zaštite u odnosu na interese pogođenih pojedinaca*. To znači da bi trebalo uraditi test ravnoteže interesa i preduzeti adekvatne tehničko-organizacione mere zaštite.

- ✓ *Ako je obrada neophodna za potrebe preventivne medicine ili medicine rada* zbog procene radne sposobnosti zaposlenih, medicinske dijagnoze, pružanja zdravstvene ili socijalne zaštite ili lečenja ili upravljanja sistemima i uslugama zdravstvene ili socijalne zaštite na osnovu prava Unije ili prava države članice ili u skladu sa ugovorom sa zdravstvenim radnikom i shodno uslovima i merama zaštite iz stava 3;

Dopuštenost obrade podataka po ovom osnovu se odnosi uglavnom na zdravstvene podatke *zaposlenih u cilju unapređenja zdravstvenog stanja zaposlenih. Ako je obrada neophodna za potrebe preventivne medicine ili medicine rada regulisani su posebni zahtevi za stručnjake koji ih obrađuju.* Stručnjaci moraju da budu obavezani čuvanjem profesionalne tajne *(čl. 9 st. 3 OUZP), koja je utvrđena pravom EU ili države članice ili nadležna nacionalna tela.*

- ✓ *Ako je obrada neophodna iz razloga javnog interesa u oblasti javnog zdravlja*, kao što je zaštita od ozbiljnih prekograničnih pretnji za zdravlje ili obezbeđivanje visokih standarda kvaliteta i bezbednosti zdravstvene zaštite i lekova i medicinskih sredstava, na osnovu prava Unije ili prava države članice kojim se propisuju odgovarajuće i posebne mere za zaštitu prava i sloboda lica na koje se podaci odnose, a posebno čuvanje profesionalne tajne;

U slučaju potrebe iz razloga javnog zdravlja, ako je to neophodno mogu se obrađivati zdravstveni podaci. Pritom je neophodno da se bliži uslovi odrede pravom EU ili pravom država članica i da se preduzmu adekvatne mere zaštite, *a* posebno čuvanje profesionalne tajne.

- ✓ *Ako je obrada neophodna za potrebe arhiviranja u javnom interesu, potrebe naučnog ili istorijskog istraživanja ili statističke potrebe* u skladu sa članom 89, stav 1. na osnovu prava Unije ili prava države članice koje

je srazmerno željenom cilju i kojim se poštuje suština prava na zaštitu podataka i obezbeđuju primerene i posebne mere za zaštitu osnovnih prava i interesa lica na koje se podaci odnose.

Obrada osetljivih podataka u svrhe arhiviranja u javnom interesu, potrebe naučnog ili istorijskog istraživanja ili statističke potrebe takođe predstavlja jedan od mogućih uslova dopuštenosti. Države članice EU ili pravom EU se mogu regulisati dalji uslovi ovih obrada. Pritom je neophodno da se poštuje suština prava zaštite podataka*, odnosno njegova načela (čl. 5 OUZP). Uz to drugi kriterijum je* obezbeđivanje adekvatnih mera zaštite u odnosu na interese pogođenih pojedinaca*. To znači da bi trebalo uraditi test ravnoteže interesa i preduzeti adekvatne tehničko-organizacione mere zaštite.*[166]

Obrada osetljivih podataka u drugim slučajevima osim navedenih nije dozvoljena. Zakonske osnove obrade osetljivih podataka su naglašene i nedvosmisleno proizlaze iz načela zakonitosti obrade (U.t.r 51 OUZP). Kategorije osetljivih podataka inače po sebi imaju *veći intenzitet osetljivosti* u odnosu na ostale podatke o ličnosti i predstavljaju po sebi *veći stepen rizika* za pojedince. Zbog toga su postavljeni stroži zahtevi u pogledu mogućnosti zadiranja u prava pojedinaca. To naravno ne znači da je čl. 9 OUZP potisnuo zahteve iz čl. 6 OUZP, već on *predstavlja dodatne uslove dopuštenosti zakonite obrade podataka koji moraju da budu ispunjeni u odnosu na čl. 6 OUZP.*

Automatske odluke koje se baziraju na osetljivim podacima su dopuštene takođe ukoliko je pogođeno lice dalo izričit pristanak ili se radi o specijalnom pravnom osnovu i obrada je neophodna radi sprovođenja značajnog javnog interesa (čl. 22 st. 4 OUZP).

Rukovaoci koji obrađuju osetljive podatke su svakako *u obavezi da vode evidenciju aktivnosti obrade podataka* (čl. 30 st. 5 OUZP).

U slučaju *masovne obrade oseljivih podataka* mora se *sprovoditi procena uticaja u vezi sa zaštitom podataka* (čl. 35 st. 3 b) OUZP).

Takođe u slučaju masovne obrade osetljivih podataka i ako se obrada sprovodi kao osnovna delatnost rukovaoca ili obrađivača, *neophodno je imenovanje ovlašćenog lica za zaštitu podataka* (čl. 37 st. 1 c) OUZP).[167]

---

[166] Kammer für Arbeiter und Angestellte für Wien, Frequently asked questions (FAQ) zur Datenschutz-Grundverordnung, 20.05.2018., str. 13, 14.

[167] Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, Kurzpapier Nr. 17: Besondere Kategorien personenbezogener Daten, https:// www. datenschutzzentrum. de/ artikel/ 1216-Kurzpapier-Nr.-17-Besondere-Kategorien-personenbezogener-Daten.html, 01.11.2018.

5. PRAVO NA OBAVEŠTENOST POJEDINACA

5.1. Opšta pravila za transparentne informacije, komunikaciju i modalitete za ostvarivanje prava pojedinaca (čl. 12 OUZP)

Informacije (čl. 12 st. 1 OUZP), koje se pružaju pojedincima moraju biti:

- ✓ koncizne, transparentne, razumljive i lako dostupne;
- ✓ jasne i uz upotrebu običnog jezika;
- ✓ posebno jasne i uz upotrebu običnog jezika za pružanje informacija deci;
- ✓ u pisanoj formi „ili uz pomoć drugih sredstava, uključujući kada je to prikladno, elektronskim putem";
- ✓ kada to zatraži pojedinac, dostavljene usmeno; i
- ✓ besplatne (čl. 12 st. 5 OUZP).

Koncizne, transparentane, razumljive i lako dostupane informacije podrazumevaju da rukovaoci treba efikasno i sažeto da prezentuju informaciju kako bi *izbegli zamor informacijama*.

Informacije koje se pružaju pojedincima, *treba jasno razlikovati od drugih informacija* koje se ne odnose na zaštitu podataka, kao što su ugovorne odredbe ili opšti uslovi poslovanja/korišćenja.

PRIMER slojevite izjave o zaštiti podataka / obaveštenja o zaštiti podataka
U onlajn okruženju korišćenje slojevitih izjava o zaštiti podataka / obaveštenja o zaštiti podataka. Ova metoda omogućava pojedincu da se kreće do određenog dela izjave o zaštiti podataka / obaveštenja o zaštiti podataka, koji ga interesuje. Na taj način je pojedinac u mogućnosti da odmah pristupi željenom sadržaju, a ne da se kreće kroz obiman tekst za konkretna pitanja. *Prvi sloj* treba da sadrži *detalje o svrsi obrade, identitet rukovaoca i opis prava pojedinca*. To su informacije do za koje odmah treba skrenuti pažnju pojedincima (npr. onlajn obrazac). Prvi sloj takođe treba da sadrži i *podatke o obradi koja ima najveći uticaj na subjekta podataka* i samu obradu, koja bi mogla iznenaditi pojedince.

Razumljivost informacije se odnosi na to da informacije treba da budu razumljive za prosečnog člana ciljane publike. Pri ostvarivanju ovog zahteva treba obratiti pažnju, koji pojedinci primaju informacije. Tako se različita informacija pruža radnicima u nekoj firmi u odnosu na informacije, koje se saopštavaju deci. Ovaj zahtev je usko povezan sa zahtevom da se koristi jasan i običan jezik.[168]

Lako pristupačane informacije znači da pojedinac ne bi trebalo da traži informacije, već odmah može da pristupi željenim informacijama.

---

[168] Radna grupa član 29, Article 29 Working Party, *Vodič u vezi sa transparentnošću pod OUZP*, Guidelines on transparency under Regulation 2016/679, 17/EN, WP260 rev.01, 11.4.2018., str. 7.

PRIMERI LAKO PRISTUPAČNE INFORMACIJE
Direktno pružanje informacija, upućivanje linkovima, jasno obeležavanje, slojevite izjave o privatnosti, najčešće postavljana pitanja „FAQ“, iskačući prozori „baneri“, koji se aktiviraju kada pojedinac popunjava onlajn formular.

PRIMER APLIKACIJE LAKO PRUŽANJE INFORMACIJA
Kod aplikacija, neophodne informacije bi trebalo da budu lako dostupne u onlajn prodavnici pre preuzimanja. Kada se aplikacija instalira, informacije moraju biti dostupne u okviru aplikacije. Jedan od načina za ispunjavanje ovog zahteva je da se osigura da informacije budu dostupne tako da za pristup nikada ne bude potrebno više od dva poteza. Pored toga, informacije o privatnosti treba da budu specifične za određenu aplikaciju i ne bi trebalo da budu samo uopštena politika privatnosti kompanije koja poseduje aplikaciju ili je stavlja na raspolaganje javnosti.

PRIMER KONTROLNA TABLA PRIVATNOSTI
Kontrolna tabla privatnosti predstavlja jedinstveno mesto, gde pojedinci mogu da pregledaju informacije o privatnosti i upravljaju svojim podacima. Pojedinci su u mogućnosti da dozvole ili spreče da se njihovi podaci koriste na određene načine za određene usluge. Ovo je naročito korisno kada pojedinci koriste istu uslugu na različitim uređajima jer im omogućava pristup i kontrolu svojih ličnih podataka, bez obzira na to kako koriste uslugu. Upotreba kontrolne table za privatnost u ponuđenim uslugama je poželjno jer se i na taj način ostvaruje princip privacy by design i privacy by default.

Uslov da *jezik bude jasan i običan* je potrebno primeniti pri formulisanju informacija zavisno od načina pružanja (pisano, usmeno, audio-vizuelno, video). Zahtev za jasnim i jednostavnim jezikom znači da se informacije moraju pružati na što jednostavniji način, izbegavajući složene rečenice i jezičke strukture (U.t.r. 42 OUZP). Informacije bi trebale biti konkretne i nedvosmislene, ne bi trebalo da budu u apstraktnom ili dvosmislenom obliku ili da ostavljaju prostor za drugačije tumačenje. Posebno treba da bude *jasna svrha i zakonski osnov obrade podataka*. Informacije dostavljene pojedincima ne bi trebalo da sadrže previše pravni, tehnički ili stručni jezik ili terminologiju.

Informacije treba pružati *pisano ili na drugi način*. Pisana forma je pravilo ali je omogućena takođe upotreba drugih sredstva uključujući i elektronska sredstva.

PRIMER ELEKTRONSKA SREDSTVA
Upotreba slojevitih izjava o zaštiti podataka / obaveštenja o zaštiti podataka, koja omogućavaju posetiocima sajta navigaciju na određene relevantne aspekte u izjavi / obaveštenju koje su bitne za njih. Potrebno je da bude upućena celina informacija i da informacije posetiocima budu na raspolaganju na jednom mestu ili u jednom kompletnom dokumentu (bilo u digitalnom ili papirnom formatu), kojem se može lako pristupiti.

PRIMER DRUGA ELEKTRONSKA SREDSTVA
Iskačući prozori (pop-up obaveštenja) i kontrolne table za privatnost.[169]

PRIMER DRUGA NEELEKTRONSKA SREDSTVA
Dodatak slojevitoj izjavi o zaštiti podataka / obaveštenju o zaštiti podataka mogu uključivati video zapise ili glasove upozorenja na mreži. Ostala sredstva, koja nisu nužno elektronska, mogu uključivati crtaće, grafičke, piktogramske ili dijagramske oznake. Za decu mogu to biti stripovi, crtani filmovi, animacije.

Važno za princip transparentnosti je da on nije ograničen samo na jezičke komunikacije u pisanom ili usmenom obliku, već je to svakako moguće i u onlajn okruženju (veb sajt, aplikacije itd.). Takođe *alate za vizuelizaciju* (slikovni simboli, piktogrami, mehanizmi sertifikacije, pečati i oznake za zaštitu podataka), treba upotrebiti gde je to prikladno (U.t.r. 58 OUZP). Alate za vizuelizaciju treba primeniti posebno kada se radi dostupnosti informacija upućenih javnosti ili pojedincima u onlajn okruženju.

Informacije mogu biti pružene i u kombinaciji sa standardizovanim slikovnim simbolima, čime se omogućava višeslojni pristup. Čl. 12 st. 7 OUZP podstiče primenu slikovnih simbola: „Informacije koje se pružaju pojedincima u skladu sa članovima 13. i 14. mogu se pružiti u kombinaciji sa standardizovanim slikovnim simbolima, kako bi se na lako vidljiv, razumljiv i jasno čitljiv način pružio smislen pregled nameravane obrade. Ako su slike prikazane elektronskim putem, one moraju biti čitljive za mašine". *Primena slikovnih simbola ne sme služiti kao zamena za pružanje informacija*, već služi kao *dodatni element transparentnosti prema pojedincima*. Pravi cilj korištenja slikovnih simbola je smanjivanje velikih i obmnih tekstova pojedinacima.[170]

Informacije se mogu dostaviti usmeno pojedincu na zahtev, pod uslovom da se njihov identitet može dokazati. Zahtev da se potvrdi identitet pojedinca pre nego što se usmeno pruži informacija se primjenjuje samo na informacije koje se odnose na prava subjekata iz čl. 15-22 i 34 OUZP. Ovaj *uslov za davanje usmenih informacija se ne može primeniti* na pružanje opštih informacija o zaštiti podataka vezano za *čl. 13 i 14 OUZP*, jer ove informacije moraju biti dostupne i budućim korisnicima/kupcima (čiji identitet rukovalac nije u mogućnosti da proveri). Informacije iz čl. 13 i 14 OUZP se mogu obezbediti usmeno, bez zahteva za identifikacijom pojedinaca.

Rukovaoci generalno ne smeju da naplaćuju pružanje informacija (čl. 12 st. 5 OUZP). *Informisanje pojedinaca* (čl. 13 i 14, 15-22 i 34 OUZP) je *besplatno* i ne sme biti uslovljeno finansijskim transakcijama.

Rukovaoci pri komunikaciji ukoliko dođe do *povrede bezbednosti podataka* moraju u potpunosti uzeti u obzir navedene opšte zahteve transparentnosti (čl. 12 OUZP). Obaveštavanje pojedinaca o povredama bezbednosti podataka (čl. 34 OUZP) mora da zadovolji opšte zahteve naročito u pogledu upotrebe jasnog i jednostavnog jezika.[171]

---

[169] *Ibidem*, str. 8, 10, 11, 12.

[170] *Ibidem*, str. 22.

[171] *Ibidem*, str. 33.

Da bi *pojedinci* mogli da ostvare svoja *prava* iz čl. 15-20 OUZP, neophodno je da rukovalac može da utvrdi njihov *identitet*. Postoji mogućnost da *rukovalac pojedinca ne može identifikovati*, pošto njegova identifikacija nije neophodna za ostvarivanje svrhe obrade podataka. U tom slučaju on *nije u obavezi da identifikuje pojedinca* (čl. 11 st. 1 OUZP). Ovaj zahtev stoji usko u vezi sa načelom minimizacije podataka. O nemogućnosti identifikacije rukovalac je dužan da *obavesti pojedinca*, koji može *dostaviti dodatne informacije* da bi dokazao svoj identitet (čl. 11 st. 2 OUZP). Rukovalac *ne sme da odbije vršenje prava pojedinaca*, već *mora da dokaže da nije u stanju da identifikuje pojedinca* (čl. 12 st. 2 OUZP). Ukoliko postoji kod rukovaoca *opravdana sumnja u pogledu identiteta pojedinca*, rukovalac *može tražiti od pojedinca dodatne informacije radi identifikacije* (čl. 12 st. 6 OUZP). *Opravdana sumnja u pogledu identeta* može postojati, ako je pojedinac podneo zahtev usmeno ili ako je podneo zahtev putem e-maila a ime i prezime nisu jasni.[172]

Stiče se utisak da će u praksi morati da dođe do ispitivanja srazmernosti u između prava pojedinca i napora rukovaoca da identifikuje pojedinca. Pored toga bitno je uočiti i to da za čl. *12-14 OUZP nije potrebna identifikacija pojedinaca*. Takođe *vršenje prava pojedinaca iz čl. 21 i 22 OUZP nije uslovljeno njihovom identifikacijom.* Dodatna identifikacija je više svedena na mogućnost, a ne na to da je rukovalac u obavezi da je izvrši. Ipak potrebno je od slučaja do slučaja proceniti, da li je identifikovanje neophodno i srazmerno.

U pogledu ostvarivanja prava pojedinaca bitno je *obratiti pažnju na rokove***.** Rukovalac mora *bez odlaganja* da odgovori pojedincima na zahtev za ostvarivanje njihovih prava (15-22 OUZP), a *najkasnije* mora da odgovori *u roku od mesec dana*. Kod *kompleksnih slučajeva* i ako postoji *veliki broj zahteva*, rok od mesec dana se može *produžiti* za još najduže *dva meseca*. Rukovalac je tada u obavezi da *obavesti pojedince o produžetku u roku od mesec* dana od prijema zahteva *zajedno sa razlozima za odlaganje* (čl. 12 st. 3 OUZP).

Rukovaoci imaju dakle:

- ✓ obavezu da odgovore na zahtev pojedinca u roku od najkasnije *mesec dana* (za *uobičajene zahteve*); ili
- ✓ obavezu da odgovore na zahtev u roku od maksimalno *3 meseca (kod kompleksnih slučajeva* i ako postoji *veliki broj zahteva*).

Ako rukovalac odbije zahtev pojedinca, on je u obavezi *u roku od mesec* dana od prijema zahteva, da *obavesti* pojedinca *o razlozima* odbijanja zahteva, o *daljim mogućnostima žalbe* nadzornom organu ili tužbe nadležnom sudu.

[172] Ursula Illibauer, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 117, 118.

5.2. Informacije koje treba saopštiti ako se podaci prikupljaju od pojedinca (čl. 13 OUZP)

Informacije koje se pružaju pojedincima, kada se direktno podaci od njih prikupljaju zahtevaju odgovarajuću formu. Obaveštenje sa takvim informacijama se često naziva *obaveštenje o zaštiti podataka, obaveštenje o privatnosti, politika privatnosti, izjava o privatnosti* ili *obaveštenje o pravičnoj obradi* (identično važi i za informacije iz čl. 14 OUZP). Obaveštenja o zaštiti podataka treba razlikovati od uslova za punovažan pristanak na obradu podataka, iako su informacije iz čl. 13 i 14 OUZP su integralni deo forme pristanka.

OUZP ne propisuje format ili modalitet kojim se informacije (čl. 13 i 14 OUZP) trebaju dostaviti pojedincu. Odgovornost rukovaoca je da preduzme odgovarajuće mere u vezi sa pružanjem potrebnih informacija u cilju ostvarenja principa transparentnosti. To znači da rukovalac treba da uzme u obzir sve okolnosti prikupljanja i obrade podataka prilikom odlučivanja o odgovarajućem modalitetu i formatu pružanja informacija. Preporučuje se da, ako rukovalac prikuplja podatke putem interneta, treba on da obezbedi da izjava o privatnosti bude na internetu.

Mogući načini prikupljanja podataka od strane rukovaoca, kada se podaci prikupljaju od pojedinaca su:

- ✓ kada pojedinac svesno pruža podatke o ličnosti rukovaocu (npr. putem online formulara); ili
- ✓ kada rukovalac prikuplja podatke od pojedinca putem nadzora (npr. pomoću automatskih uređaja za snimanje podataka ili kamera, mrežne opreme, Wi-Fi praćenja, RFID ili druge vrste senzora).

U pogledu vremena pružanja informacija, *informacije se moraju dostaviti u vreme kada se prikupljaju lični podaci* (čl. 13 st. 1 OUZP).

Ukoliko dođe do *promene svrhe obrade podataka* (čl. 13 st. 3 OUZP) treba izvršiti *promene u izjavi o privatnosti / obaveštenju o zaštiti podataka* i *dostaviti dodatne informacije* pojedincima, koje su promenjene. Dodatno informisanje treba izvršiti posebno ako su se desile sledeće promene: *promena svrhe obrade, promena identiteta rukovaoca, promena prirode obrade* (npr. proširenje kategorija primalaca ili prenos u treću zemlju), *promene u pogledu toga kako pojedinci mogu ostvariti svoja prava u vezi sa obradom.* Ukoliko se radi o izmenama u vidu ispravki gramatičkih ili stilskih grešaka, tada nije neophodno informisati ponovo pojedince.

Informacije o postojanju automatizovanog odlučivanja, uključujući profilisanje (čl. 22 st. 1 i 22 st. 4 OUZP) uključujući informacije o logici i predviđenim posledicama obrade po pojedince, čini deo obaveznih informacija koje se moraju dostaviti pojedincima (čl. 13 st. 2 f) OUZP). Tom prilikom je važno *informisati*

pojedinaca o posledicama obrade njihovih ličnih podataka, kao i primeniti opšte načelo da se pojedinci ne iznenadjuju pri obradi njihovih ličnih podataka.[173]

5.3. Informacije koje treba saopštiti kada podaci nisu prikupljeni od pojedinaca (čl. 14 OUZP)

Kada podaci nisu dobijeni od pojedinaca postoje razlike u obavezama informisanja za rukovaoca. *Mogući načini prikupljanja podataka* od strane rukovaoca su:

- ✓ kada drugi rukovaoci pružaju podatke;
- ✓ kada su podaci javno dostupni;
- ✓ kada se podaci prikupljaju od prodavaca podataka; ili
- ✓ od drugih pojedinaca.

Vreme pružanja informacija, kada se podaci ne prikupljaju od pojedinaca, određeno je na sledeći način:

- ✓ Opšti uslov je da se informacije moraju dostaviti u "razumnom roku" nakon pribavljanja ličnih podataka i *najkasnije u roku od mesec dana*," imajući u vidu specifične okolnosti u kojima se obrađuju lični podaci".
- ✓ Kada se podaci koriste za komunikaciju sa pojedincem, tada informacije moraju biti pružene *najkasnije u trenutku prve komunikacije sa pojedincem*. Tada se informacije moraju pružiti pre isteka roka od mesec dana, dakle u trenutku prve komunikacije sa pojedincem.
- ✓ Opšti rok od meseca dana se može smanjiti i kada se podaci otkrivaju / objavljuju drugom primaocu (bilo trećoj strani). Tada informacije moraju biti dostavljene *najkasnije u trenutku prvog objavljivanja*. U ovom slučaju, ako se obelodanjivanje javlja pre jednomesečnog vremenskog ograničenja, tada informacije moraju biti obezbeđene najkasnije u vreme prvog objavljivanja, bez obzira na to da je istekao mesec od trenutka dobijanja podataka.

Ukoliko dođe do *promene svrhe obrade podataka* (čl. 14 st. 4 OUZP) treba izvršiti *promene u izjavi o privatnosti / obaveštenju o zaštiti podataka* i *dostaviti dodatne informacije* pojedincima, koje su promenjene. Dodatno informisanje treba izvršiti posebno ako su se desile sledeće promene: *promena svrhe obrade, promena identiteta rukovaoca, promena prirode obrade* (npr. proširenje kategorija primalaca ili prenos u treću zemlju), *promene u pogledu toga kako pojedinci mogu ostvariti svoja prava u vezi sa obradom.* Ukoliko se radi o izmenama u vidu ispravki gramatičkih ili stilskih grešaka, tada nije neophodno informisati ponovo pojedince.

---

[173] *Ibidem*,str. 13, 14, 21.

Informacije o postojanju automatizovanog odlučivanja, uključujući profilisanje (čl. 22 st. 1 i 22 st. 4 OUZP) sa informacijama o logici i predviđenim posledicama obrade po pojedince, čini deo obaveznih informacija koje se moraju dostaviti pojedincima (čl 14 st. 2 g) OUZP). Tom prilikom je važno *informisati pojedinaca o posledicama obrade njihovih ličnih podataka*, kao i primeniti opšte načelo da se pojedinci ne iznenadjuju pri obradi njihovih ličnih podataka.[174]

5.4. Sadržaj informacija koje se moraju saopštiti pojedincima (čl. 13 i 14 OUZP)

Informacije koje se moraju saopštiti pojedincima shodno čl. 13 i 14 OUZP		
Zahtevana informacija	*Čl. 13 OUZP*	*Čl. 14 OUZP*
Ime i kontakt podaci rukovaoca	Čl. 13 st. 1 (a)	Čl. 14 st. 1 (a)
Gde je primenljivo, kontakt podaci ovlašćenog lica za zaštitu podataka	Čl. 13 st. 1 (b)	Čl. 14 st. 1 (b)
Svrha, u koju se podaci obrađuju	Čl. 13 st. 1 (c)	Čl. 14 st. 1 (c)
Pravni osnov obrade podataka	Čl. 13 st. 1 (c)	Čl. 14 st. 1 (c)
Kada se radi o pravnom osnovu „opravdanog interesa“, navodi o opravdanim interesima rukovaoca	Čl. 13 st. 1 (d)	Čl. 14 st. 2 (b)
Kategorije ličnih podataka, koje se obrađuju	Nije neophodno	Čl. 14 st. 1 (d)
Gde je moguće, primaoci ili kategorije primalaca podataka o ličnosti	Čl. 13 st. 1 (e)	Čl. 14 st. 1 (e)
Gde je moguće, informacije o transferu podataka u treće zemlje	Čl. 13 st. 1 (f)	Čl. 14 st. 1 (f)
Period čuvanja podataka o ličnosti. Kada to nije moguće, kriterijumi za određivanje perioda	Čl. 13 st. 2 (a)	Čl. 14 st. 2 (a)
Postojanje prava na informaciju, ispravku, brisanje, ograničenje obrade, prigovor i prenosivost podataka	Čl. 13 st. 2 (b)	Čl. 14 st. 2 (c)
Postojanje prava na opoziv, kada se obrada zasniva na pristanku	Čl. 13 st. 2 (c)	Čl. 14 st. 2 (d)
Postojanje prava na žalbu nadzornom organu za zaštitu podataka	Čl. 13 st. 2 (d)	Čl. 14 st. 2 (e)

[174] *Ibidem*, str. 21.

Informacije koje se moraju saopštiti pojedincima shodno čl. 13 i 14 OUZP		
Zahtevana informacija	*Čl. 13 OUZP*	*Čl. 14 OUZP*
Da li je pružanje podataka o ličnosti zakonska ili ugovorna obaveza ili nužan uslov za sklapanje ugovora. Da li pojedinac ima obavezu pružanja podataka o ličnosti i koje su moguće posledice ako se ti podaci ne pruže	Čl. 13 st. 2 (e)	Nije neophodno
Informacije o izvorima iz kojih potiču podaci o ličnosti i gde je to moguće, da li podaci potiču iz javno dostupnih izvora	Nije neophodno	Čl. 14 st. 2 (f)
Postojanje automatskih odluka uključujući profilisanje, kao i informacije o upotrebljenoj logici, domašaju i posledicama obrade podataka	Čl. 13 st. 2 (f)	Čl. 14 st. 2 (g)
U slučaju dalje obrade (sve relevantne informacije shodno čl. 13 st. 2 ili čl. 14 st. 4)	Čl. 13 st. 3	Čl. 14 st. 4

5.5. Informacije koje se ne moraju saopštiti pojedincima (čl. 13 i 14 OUZP)

Informacije koje se ne moraju saopštiti pojedincima shodno čl. 13 i 14 OUZP		
Izuzeci od prava na informaciju	*čl. 13 OUZP*	*čl. 14 OUZP*
Pojedinci ne moraju biti informisani, ukoliko su već informisani	Čl. 13 st. 4	Čl. 14 st. 5 (a)
Kada je pružanje informacija nemoguće ili bi zahtevalo nerazmerne napore. To važi naročito za obrade u svrhu arhiviranja u javnom interesu, u svrhu naučnog ili istorijskog istraživanja ili u statističke svrhe	Nije neophodno	Čl. 14 st. 5 (b)
Dobijanje ili otkrivanje podataka regulisano pravom EU ili pravom države članice	Nije neophodno	Čl. 14 st. 5 (c)
Kada podaci o ličnosti podležu obavezi čuvanja profesionalne tajne (uključujući obavezu čuvanja tajne koja se navodi u statutu) moraju ostati poverljivi	Nije neophodno	Čl. 14 st. 5 (d)

Izuzeci od pružanja informacija pojedincima, *pored izuzetka kada su informacije već pružene pojedincima*, dopušteni su:

- ✓ Ako je *obezbeđivanje informacija nemoguće ili bi zahtevalo nerazmerne napore*, posebno za obrade u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, ili gde bi ciljeve obrade postali nemogući ili ozbiljno ugroženi;
- ✓ Kada rukovalac *podleže nacionalnom zakonu ili pravu EU*, ako pribavi ili otkrije lične podatke i kada zakon pruža odgovarajuću zaštitu za legitimne interese pojedinaca; ili
- ✓ Kada se radi o *obavezi čuvanja profesionalne tajne* (uključujući zakonsku obavezu tajnosti) koja je regulisana nacionalnim ili evropskim zakonom. Tada lični podaci moraju ostati poverljivi.

Prvi izuzetak od pružanja informacija pojedincima zahteva od rukovaoca dokaže 1 od 3 situacije:

- ✓ tamo gde se to pokazuje nemogućim (posebno za arhiviranje, naučna/ istorijska istraživanja ili statističke svrhe);
- ✓ gde bi to uključivalo nesrazmerne napore (posebno za arhiviranje, naučna/ istorijska istraživanja ili statističke svrhe); ili
- ✓ kada bi pružanje informacija moglo ozbiljno narušiti postizanje ciljeva obrade ili bi ostvarivanje ciljeva obrade postalo nemoguće.[175]

„Nemogućnost pružanja informacije“ - Ako rukovalac želi da se osloni na ovaj izuzetak, mora da dokaže faktore koji ga sprečavaju da pruži informacije pojedincima. Ako protekom određenog vremenskog perioda, faktori koji su prouzrokovali nemogućnost više ne postoje, tada treba pružiti informacije pojedincima.

PRIMER NEMOGUĆNOST PRUŽANJA INFORMACIJA
Korisnik se registruje na onlajn pretplatnički servis. Nakon registracije, rukovalac prikuplja kreditne podatke agencije za kreditno izveštavanje o korisniku, kako bi odlučio da li će pružiti uslugu. Rukovalac mora da informiše korisnika o prikupljanju ovih podataka o kreditu u roku od mesec dana od prikupljanja (shodno čl. 14 st. 3 a) OUZP). Međutim, adresa i telefonski broj korisnika nisu upisani u javne registre (osoba živi u inostranstvu). Korisnik nije ostavio e-mail prilikom registracije za uslugu ili je e-mail adresa nevažeća. Rukovalac zaključuje da nema sredstava direktnog kontakta sa korisnikom. U ovom slučaju je nemoguće pružiti informacije u skladu sa čl. 14. Međutim, i u ovom slučaju rukovalac može dati informacije o prikupljanju podataka o kreditnom izveštavanju na svojoj veb stranici pre same registracije.

[157] *Ibidem*, str. 27.

Nemogućnost pružanja izvora podataka (U.t.r. 61 OUZP)„ukoliko se izvor podataka o ličnosti ne može dati pojedincu jer su upotrebljavani razni izvori, trebalo bi dati opšte informacije". Uskraćivanje zahteva za pružanje informacija pojedincima o izvorima njihovih ličnih podataka primjenjuje se samo tamo gde to nije moguće, kada se različiti delovi ličnih podataka koji se odnose na istog pojedinca ne mogu pripisati određenom izvoru. Sama činjenica da baza podataka sadrži lične podatke više osoba sa podacima koje koristi više izvora, nije dovoljna ispunjenje ovog zahteva, ako je moguće (iako je potrebno vreme ili dodatni napor) identifikovati izvor iz kojeg su izvedeni lični podaci pojedinaca.

„Nesrazmerni napor" se može primeniti za obradu u svrhe arhiviranja u javnom interesu, za naučno / istorijske istraživačke svrhe ili statističke svrhe. U.t.r. 62 OUZP se odnosi na ove ciljeve i u pogledu nesrazmernog napora treba uzeti u obzir sledeće faktore: *broj pojedinaca, starost podataka i odgovarajuće zaštitne mere*.

PRIMER NESRAZMERNI NAPORI
Istoričari u svom istraživanju žele da istraže prezimena u određenom istorijskom kontekstu. Tom prilikom indirektno dobijaju podatke od 50.000 pojedinaca. Ovi podaci su prikupljeni pre 50 godina, nisu ažurirani od tada i ne sadrže nikakve kontakt podatke. S obzirom na obim i starost podataka, pojedinačno obaveštavanje pojedinaca shodno čl. 14 OUZP u ovom slučaju bi uključivalo nesrazmerne napore za istraživače.

Ako rukovalac pokuša da se osloni na izuzetak, na osnovu koga bi tvrdio da je pružanje informacija uključilo nesrazmerne napore, trebao bi najpre *ispitati proporcionalnost u odnosu na prava pojedinaca*. Tom prilikom potrebno je proceniti *napor koji je potreban za rukovaoca da pruži informacije pojedincu nasuprot uticaju i efektu na pojedinca ako mu nije pružena informacija.* Ovu procenu treba rukovalac da dokumentuje. Pored toga rukovalac mora preduzeti odgovarajuće mere za zaštitu prava, sloboda i legitimnih interesa pojedinaca. Ovaj zahtev se primenjuje i onda kada rukovalac utvrdi da pružanje informacija nije moguće, ili bi verovatno onemogućilo ili ozbiljno ugrozilo postizanje ciljeva obrade. Jedna od odgovarajućih mera je da informacije budu javno dostupne npr. stavljanjem informacija na svoju veb stranicu ili proaktivnim oglašavanjem informacija u novinama.

„Ozbiljno narušavanje ciljeva" podrazumeva da rukovaoci moraju pokazati da bi pružanje informacija samo poništilo ciljeve obrade.[176]

Drugi izuzetak od pružanja informacija pojedincima postoji, ukoliko je pribavljanje ili obelodanjivanje ličnih podataka izričito propisano zakonom EU ili države članice. Ovaj izuzetak je takođe uslovljen obezbeđivanjem odgovarajućih mera za zaštitu legitimnih interesa pojedinaca. Rukovalac mora da pokaže kako se predmetni zakon odnosi na njega i da zahteva od njega da dobije ili otkrije lične podatke. Pored toga treba da bude u stanju da demonstrira da je pribavljanje ili otkrivanje ličnih podataka su u skladu sa zakonom.

[176] *Ibidem*, str. 28, 29, 30.

PRIMER ZAKONSKO REGULISANO PRIBAVLJANJE PODATAKA
Poreski organi podležu obavezi po nacionalnom zakonu da dobiju detalje o platama zaposlenih od strane njihovih poslodavaca. Lični podaci se ne dobijaju od pojedinaca i prema tome poreski organ podleže zahtevima člana 14. Pošto je pribavljanje ličnih podataka od strane poreskog organa od poslodavaca izričito propisano zakonom, stoga se zahtevi za informacije iz člana 14 u ovom ne primenjuju na poreske organe.

Treći izuzetak od pružanja informacija pojedincima „Poverljivost na osnovu obaveze tajnosti" postoji, ukoliko postoji kada lični podaci moraju ostati poverljivi, kada podležu obavezama čuvanja profesionalne tajnosti regulisane zakonom EU ili države članice, uključujući i zakonsku obavezu tajnosti za rukovaoce. Ako rukovalac pokušava da se osloni na ovaj izuzetak, on mora biti u stanju da dokaže i pokaže kako se obaveza profesionalne tajne direktno odnosi na rukovaoca tako što mu zabranjuje da pruži informacije pojedincima.[28]

[28] *Ibidem,* str. 31, 32.

6. PRAVA POJEDINACA

6.1. Pravo na pristup podacima (čl. 15 OUZP)

U pravu zaštite podataka pojedinci (pogođena lica) imaju samo i isključivo prava. Pravo na pristup podacima predstavlja jedno od najvažnijih prava pojedinaca. To je pre svega iz razloga što pojedinci da bi ostvarili ostala prava (iako ona formalno pravno nisu međusobno uslovljena) treba da provere koje podatke uopšte rukovaoci o njima obrađuju. Stoga se u praksi i preporučuje da pojedinci najpre podnesu zahtev za pristup podacima. Iz tih razloga je potrebno objasniti, na koji način bi ovo pravo trebalo da se ostvaruje u praksi.

U početnoj fazi pojedinac smatra da neki rukovalac obrađuje podatke o njemu. Pojedinac treba da podnese zahtev rukovaocu radi informacije, koje podatke rukovalac o njemu obrađuje. Pritom je potrebno da podnosilac zahteva podnese i kopiju nekog svog službenog dokumenta (pasoša, lične karte i sl.). Rukovalac po zahtevu treba da odgovori sa listom podataka, koje obrađuje o pojedincu odnosno podnosiocu zahteva. Tom prilikom pojedinac može konstatovati, da je njegova adresa pogrešno uneta, da su podaci promenjeni, netačni itd. Tada pojedinac može zahtevati ispravku, brisanje podataka koji su netačno ili pogrešno zabeleženi. Rukovalac postupa onda po ovom zahtevu i obaveštava o tome pojedinca.

Zahtev za pravo pristupa podacima

Pri podnošenju zahteva za pristup informacijama *pisana forma nije neophodna*. Pojedinac može podneti zahtev naravno i *pisano* i *elektronskim* putem kao i na drugi način. Informacije se mogu pružiti *usmeno*, pod uslovom da je identitet lica na koje se podaci odnose određen na druge načine (čl. 12 st. 1 OUZP). U slučaju da je zahtev podnet elektronskim putem, informacije se pružaju elektronskim putem (čl. 12 st. 3 i čl. 15 st. 3 OUZP). Osim toga *rukovalac nije u obavezi da ustanovljava identitet* podnosioca zahteva. Međutim rukovalac *može* da zahteva *dodatne informacije* neophodne za potvrđivanje identiteta lica na koje se podaci odnose, *ukoliko postoje opravdane sumnje u pogledu identiteta podnosioca zahteva* (čl. 12 st. 6 OUZP). To su situacije u praksi gde npr. neko lice telefonskim putem traži podatke o ličnosti, gde rukovalac ne zna sa kime komunicira. Takođe rukovalac ne može da odbije zahtev pojedinca, osim ako dokaže da *nije u mogućnosti da identifikuje podnosioca zahteva* (čl. 12 st. 2 OUZP).

Rokovi za podnošenje zahteva

Rukovalac treba da odgovori podnosiocu zahteva *najkasnije u roku od mesec dana od prijema zahteva*. Taj rok može prema potrebi da se *produži za dodatna dva meseca*, uzimajući u obzir složenost i broj zahteva. Rukovalac *obaveštava* lice na

koje se podaci odnose *o svakom takvom produženju u roku od mesec dana od prijema zahteva*, pri čemu navodi *razloge za odlaganje* (čl. 12 st. 3 OUZP).

Odbijanje zahteva

U slučaju da rukovalac ne postupi po zahtevu podnosioca zahteva, dužan je *da obavesti podnosioca* zahteva o tome odmah ili *najkasnije mesec dana od prijema zahteva o razlozima* zbog kojih nije postupio po zahtevu. Tom prilikom je rukovalac dužan da obavesti podnosioca zahteva *i o mogućnosti podnošenja pritužbe nadzornom organu i traženja pravnog leka.*

Razlozi odbijanja zahteva pojedinca *mogu biti u nacionalnom pravu u vidu ograničenja prava pojedinaca* (čl. 23 st. 2 h) OUZP).

Kao dalji razlozi odbijanja mogu se navesti da su *zahtevi pojedinca očigledno neosnovani ili preterani, posebno zbog toga što se često podnose* (čl. 12 st. 5 OUZP).[178]

Podaci o kojima treba izvestiti pojedince

Pod uslovom da je rukovalac u stanju da identifikuje pojedinca ili je on sam dostavio podatke o idenitifikaciji (čl. 11 st. 2 OUZP), rukovalac treba da pruži sledeće podatke (čl. 15 st. 1, 2 i 3 OUZP):

- ✓ kopiju podataka (npr. izvod i baze podataka, mejlovi itd.);
- ✓ informacije o svrsi obrade;
- ✓ podatke o kategorijama podataka o ličnosti koji u pitanju;
- ✓ podatke o korisnicima ili kategorijama korisnika kojima su podaci o ličnosti otkriveni ili će im biti otkriveni, a posebno korisnicima u trećim zemljama ili međunarodnim organizacijama;
- ✓ ukoliko je moguće, predviđenom roku u kojem će se podaci o ličnosti čuvati ili, ako to nije moguće, kriterijumima koji su korišćeni za određivanje tog roka;
- ✓ informacije o postojanju prava da se od rukovaoca zatraži pristup podacima o ličnosti i ispravka ili brisanje podataka o ličnosti ili ograničavanje obrade u vezi s licem na koje se podaci odnose i prava na prigovor na obradu;
- ✓ informacije o pravu na podnošenje pritužbe nadzornom organu;
- ✓ ako se podaci o ličnosti ne prikupljaju od lica na koje se podaci odnose, svakoj dostupnoj informaciji o njihovom izvoru;
- ✓ informacije o postojanju automatizovanog donošenja odluka, uključujući i profilisanje iz člana 22, stav 1. i 4. i, barem u tim slučajevima, sadržajne informacije logici koja se koristi, kao i značaj i predviđene posledice takve obrade za lice na koje se podaci odnose;
- ✓ ako se podaci o ličnosti prenose u treću zemlju ili međunarodnu organizaciju,

[178] Viktoria Haidinger, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 125, 126.

lice na koje se podaci odnose ima pravo da bude informisano o odgovarajućim merama zaštite u skladu sa članom 46. koje se odnose na prenos.

U slučaju da rukovalac ustanovi da *prava i slobode drugih lica* mogu biti povređena prilikom vršenja prava na pristup podacima u pogledu dostavljanja kopija podataka (čl. 15 st. 4 OUZP), tako ovi podaci ne treba da budu obuhvaćeni u odgovoru podnosiocu zahteva.

U odgovoru na zahtev rukovalac treba da povede računa o jasnoći, jednostavnosti jezika koji koristi, kao i da informacije pruži na razumljiv, pristupačan i transparentan način, a naročito ako se radi o deci (čl. 12 st. 1 OUZP).

Generalno se *odgovor na zahtev za pravo pristupa podacima ne naplaćuje* (čl. 12 st. 5 OUZP). Međutim, ukoliko pojedinac zahteva više od jedne kopije podataka, može rukovalac da odredi adekvatnu naknadu administrativnih troškova za pruženu uslugu (čl. 15 st. 3 OUZP).[179]

Pregled obaveza za rukovaoca po pravu na pristup podacima	
Forma	Sve moguće forme (pisana, usmena, elektronska itd.)
Dokaz identiteta	Samo u slučaju sumnje
Rok	Maksimalno 1 mesec od prijema zahteva (najduže 3 meseca po velikom broju zahteva i po kompleksnim zahtevima)
Podaci o kojima treba pružiti obaveštenje	✓ svrha obrade ✓ kategorija podataka ✓ korisnici ili kategorije korisnika ✓ izvor podataka (ako nisu direktno prikljupljeni od pojedinca) ✓ informacije logici koja se koristi, kao i značaj i predviđene posledice za obrade po čl. 22 st. 1 OUZP ✓ rok čuvanja podataka ✓ ostala prava pojedinaca ✓ pravo na podnošenje pritužbe nadzornom organu ✓ kod prenosa u treću zemlju ili međunarodnu organizaciju informacije o odgovarajućim merama zaštite (po čl. 46 OUZP)

[179] *Ibidem*, str. 127, 128.

6.2. Pravo na ispravljanje podataka (čl. 16 OUZP)

Pored toga što predstavlja pravo pojedinca, pravo na ispravljanje podataka predstavlja i jedno od načela zaštite podataka (čl. 5 st. 1 d) OUZP), pošto podrazumeva da su podaci tačni.

Uz to i pojedinci imaju pravo da im se bez odlaganja omogući ispravka netačnih podataka. Ukoliko pojedinac utvrdi da su određeni podaci kod rukovaoca pogrešno uneti npr. ime ili prezime ili adresa ili broj telefona itd. može zahtevati ispravku istih.

U pogledu forme, dokaza identiteta, rokova, odbijanja, troškova važe identična pravila kao i za pravo pristupa podacima.

Iako se zahteva da se podaci *bez odlaganja isprave*, potrebno je od saznanja za netačnost podataka preduzeti adekvatne mere kako bi se podaci ispravili u najkraćem mogućem roku. Takođe moguće je argumentovati i u ovom slučaju da važe opšti rokovi od mesec dana odnosno najduže 3 meseca od podnošenja zahteva.

U pogledu podataka koje treba ispraviti, rukovalac je dužan da ispravi one podatke koji su netačni. A pojedinac ima pravo *da dopuni nepotpune podatke i da da dodatnu izjavu o tome*.

Pojedinac ima pravo da *traži ograničenje obrade od rukovaoca*, ukoliko je sporna tačnost podataka, u roku kom je rukovaocu potrebno da proveri tačnosti podataka (čl. 18 st. 1 a) OUZP). Osim toga *rukovalac ima obavezu obavešavanja svakog korisnika*, *kome su podaci otkriveni* u slučaju ispravke podataka ili ograničenja obrade podataka (čl. 19 OUZP). *Pravo na obaveštavanje pojedinca o tim korisnicima* je moguće *na zahtev pogođenih pojedinaca* (čl. 19 OUZP).[180]

Pregled obaveza za rukovaoca po pravu na ispravku podataka	
Forma	Sve moguće forme (pisana, usmena, elektronska itd.)
Dokaz identiteta	Samo u slučaju sumnje
Rok	Bez odlaganja. Maksimalno 1 mesec od prijema zahteva (najduže 3 meseca po velikom broju zahteva i po kompleksnim zahtevima)
Podaci o koje treba ispraviti	Netačni podaci
Prava pojedinaca u okviru ostvarivanja prava na ispravku	Pravo dopune nepotpunih podataka i davanja dodatne izjave o tome Ograničenje obrade, ukoliko je sporna tačnost podataka (samo po zahtevu pojedinaca) Pravo na obaveštavanje o korisnicima (samo po zahtevu pojedinaca)
Obaveza obavešavanja	Svakog korisnika, kome su podaci otkriveni

[180] *Ibidem*, str. 130.

6.3. Pravo na brisanje podataka „pravo na zaborav“ (čl. 17 OUZP)

Pravo na brisanje podataka postoji u različitim slučajevima:

- ✓ *Nepostojanje prvobitne svrhe* – radi se o situaciji u kojoj prvobitni cilj obrade podataka za koji su podaci prikupljeni odpadne ili više ne postoji, pa se stoga podaci moraju obrisati. Ovo se odnosi i na situaciju, kada je cilj postugnut, pa dalje obrada podataka nije neophodna (čl. 17 st. 1 a) OUZP).

PRIMER PRESTANAK UGOVORA
Ukoliko je okončan ugovor za čije sprovođenje su podaci prikupljeni, a pritom su i istekli rokovi obaveznog čuvanja podataka, podaci o ličnosti vezani za ugovor moraju biti obrisani.

- ✓ *Povlačenje pristanka* – ukoliko se pristanak (čl. 6 st. 1 a) ili čl. 9 st. 1 a) OUZP) kao osnova obrade za koju su podaci prikupljeni povuče, ti podaci moraju biti obrisani. Izuzetak od brisanja u ovom slučaju je, kada postoji neki drugi pravni osnov za dalju obradu podataka. To bi bio slučaj npr. obaveze čuvanja podataka prema nekom zakonu (čl. 17 st. 1 b) OUZP).

PRIMER OPOZIV PRISTANKA
U slučaju kada pojedinac povuče već dat pristanka za obradu podataka kod newsletter-a. Opoziv pristanka ima dejstvo samo za budućnost. To znači da dotadašnje obrade podataka ne mogu biti naknadno proglašene nevažećim. O ovome treba da bude obavešten pojedinac prilikom davanja pristanka u okviru obaveza informisanja (čl. 13 OUZP).

Pravno gledano treba razlikovati opoziv pristanka od prigovora, koji sam predstavlja pravo pojedinca (čl. 21 OUZP).

- ✓ *Prigovor* – ukoliko pojedinac uloži prigovor kada se podaci obrađuju za izvršavanje zadatka od javnog interesa ili pri izvršavanju javne vlasti ili kada postoje opravdani interesi rukovaoca ili treće strane tada se podaci moraju obrisati (čl. 17 st. 1 c) OUZP). *Izuzetak* od prava na prigovor je predviđen u slučaju, kada *postoje pretežniji opravdani interesi* rukovaoca za dalju obradu podataka.

PRIMER PRIGOVOR PRETEŽNIJI OPRAVDANI INTERESI RUKOVAOCA
Pretežniji opravdani interesi rukovaoca za dalju obradu podataka bi postojali, kada bi na strani rukovaoca postojali pretežniji ekonomiski interesi. U tom slučaju bi ovi interesi stajali nasuprot pravu pojedinca na privatnost i zaštitu podataka. Primer takve situacije bi mogao biti kada su podaci pseudonimizovani i kada je pritom zadranje u prava pojedinaca svedeno na opravdanu meru.

Poseban slučaj predstavlja pravo na prigovor kada se podaci upotrebljavaju u svrhe direktnog marketinga, tada ne postoji izuzetak u proceni opravdanih interesa, već se podaci moraju obrisati.

PRIMER PRIGOVOR DIREKTNI MARKETING
U slučaju da određena firma šalje reklamni material poštom ili poziva u svrhe marketinga, a tom prilikom pojedinac uloži prigovor, podaci moraju biti obrisani.

- ✓ *Nezakonita obrada podataka* – ukoliko se podaci nezakonito obrađuju oni moraju biti obrisani (čl. 17 st. 1 d) OUZP). Radi se o situaciji, kada se podaci obrađuju bez pravnog osnova ili bez legitimnog pravnog osnova. U tom slučaju se savetuje da se pravni osnov obrade blagovremeno dokumentuje.
- ✓ *Izvršenje pravne obaveze* – ukoliko se podaci moraju obrisati radi ispunjenja nacionalnog prava ili prava EU (čl. 17 st. 1 e) OUZP).
- ✓ *Podaci dece* – kada su prikupljeni podaci o deci shodno čl. 8 st. 1 (čl. 17 st. 1 f) OUZP).
- ✓ *Netačni podaci* – ukoliko podaci nisu tačni treba ih obrisati (čl. 5 st. 1 d) OUZP).

Od prava na brisanje podataka postoje i određeni izuzeci, kada se *podaci ne smeju brisati:*

- ✓ *Sloboda izražavanja i informisanja* – ukoliko se podaci moraju obrađivati radi ostvarivanja prava na slobodu izražavanja i informisanja (čl. 17 st. 3 a) OUZP).

PRIMER SLOBODA IZRAŽAVANJA I INFORMISANJA
U slučaju ostvarivanja prava na slobodu izražavanja i informisanja, ne bi postojalo pravo na brisanje podataka, ukoliko bi se radilo o novinskom izveštaju, koji bi bio u javnom interesu. Takva privilegija je regulisana u Nemačkoj čl. 57 Ugovora o radio-televiziji (Runfunkstaatsvertrag).

- ✓ *Izvršenje pravne obaveze* – ukoliko se podaci moraju obrađivati radi ispunjenja nacionalnog prava ili prava EU (čl. 17 st. 3 b) OUZP).

PRIMER IZVRŠENJA PRAVNE OBAVEZE
Tipičan primer ispunjenja nacionalnog prava ili prava EU su zakonski osnovi za čuvanje podataka. Npr. u svrhe sprečavanja pranja novca, u svrhe vođenja knjiga itd.

- ✓ *Postavljanje, ostvarivanje ili obrana pravnih zahteva* – ukoliko se podaci moraju obrađivati radi postavljanja, ostvarivanja ili odbrane pravnih zahteva (čl. 17 st. 3 e) OUZP).

PRIMER ODBRANA PRAVNIH ZAHTEVA
Situacija u kojoj se neka firma nalazi u sporu sa licem, a pritom je pravni osnov obrade podataka prestao. Radi se o situaciji kada je ugovor prestao, ali lice potražuje naknadu štete. U tom slučaju tužena firma može da obrađuje podatke lica u svrhu odbrane od tužbenih zahteva.

- ✓ *Javno zdravlje* – ukoliko se podaci moraju obrađivati svrhe javnog zdravlja (čl. 17 st. 3 c) OUZP).

PRIMER JAVNO ZDRAVLJE
Situacija u kojoj se stanovništvo mora informisati o epidemiji.

- ✓ *Arhiviranje u javnom interesu, naučno istraživanje, statistika* – ukoliko se podaci moraju obrađivati svrhe javnog arhiviranja, naučnog istraživanja, statistike (čl. 17 st. 3 c) OUZP).[181]

PRIMER ARHIVIRANJE U JAVNOM INTERESU
Situacija u kojoj se obrađuju podaci o ličnosti, koji su od izuzetnog istorijskog značaja (npr. politički akteri, zasedanja Vlade).

PRAVO NA BRISANJE PODATAKA	*BEZ PRAVA NA BRISANJE PODATAKA*
Nepostojanje/ispunjenje prvobitne svrhe	Sloboda izražavanja i informisanja
Povlačenje pristanka	Izvršenje pravne obaveze (EU, domaće pravo)
Uložen prigovor	Odbrana pravnih zahteva
Nezakonita obrada podataka	Javno zdravlje
Izvršenje pravne obaveze (EU, domaće pravo)	Arhiviranje u javnom interesu, naučno istraživanje, statistika
Podaci dece	
Netačni podaci	

Obaveza rukovaoca je da bez nepotrebnog odlaganja i u svakom slučaju u roku od mesec dana od prijema zahteva odgovori pojedincu. Stoga *bez nepotrebnog odlaganja* treba tumačiti, kao bez odugovlačenja. To bi značilo da rukovalac ima dovoljno vremena da ispita predpostavke za ispunjenje zahteva, ali da mora da odgovori pojedincu u roku od mesec dana, da li će pozitivno odgovoriti na njegov zahtev (ćl. 12 st. 3 OUZP).

Obaveza rukovaoca je da kada su podaci *javno* objavljeni informiše ostale rukovaoce da je pojedinac zatražio da se svi podaci obrišu o njemu uključujući i linkove i ostale kopije podataka. Tom prilikom je rukovalac dužan da uzme u obzir dostupnu tehnologiju, trošak implementacije, proporcionalne mere, uključujući tehničke mere, kako bi ispunio ovu obavezu (čl. 17 st. 2 OUZP). Upravo ova obaveza rukovaoca se pre svega odnosi na internet u vidu "prava na zaborav". Inače *pravo na*

[181] Simone Rosenthal, Felix Bonstein, Wegradiert, *DSGVO – Datenlöschung*, EU- DSGVO konkret, IX Magazin für professionelle Informationsrechnik, 2018., str. 45.

zaborav je uspostavljeno odlukom Evropskog suda u slučaju Gugl protiv Španije.[182] Po ovoj odluci je Gugl obavezan da obriše ne samo linkove nego i sadržaje iz svog pretraživača. Pritom je važno da sadržaji dosežu do daleko u prošlost i da ličnosti iz javnog života nisu time kompromitovane. Takođe u presudi je ustanovljeno da se pojedinci mogu direktno obratiti sa ovim zahtevom Guglu ili bilo kom drugom internet pretraživaču.[183]

Ukoliko podaci *nisu javno* objavljeni, već prosleđeni ograničenom krugu primalaca, tada mora rukovalac da *informiše primaoce o brisanju podataka* (čl. 19 OUZP). Jedini izuzetak bi bio kada je to nemoguće ili kada je nesrazmerno komplikovano.[184] *Pravo na obaveštavanje pojedinca o tim korisnicima* je moguće *na zahtev pogođenih pojedinaca* (čl. 19 OUZP).

U slučaju da se *podaci nezakonito obrađuju*, pojedinac može od rukovaoca zahtevati umesto brisanja *ograničenje obrade podataka* (čl. 18 st. 1 b) OUZP).

U slučaju da je pojedinac *uložio prigovor* (po čl. 21 st. 1 OUZP), pojedinac može od rukovaoca zahtevati *ograničenje obrade podataka* (čl. 18 st. 1 d) OUZP) ukoliko još nije potvrđeno da li legitimni razlozi rukovaoca preovlađuju nad razlozima lica na koje se podaci odnose.

U slučaju da rukovaocu *dalja obrada nije potrebna* (shodno čl. 17 st. 1 a) i čl. 5 st. 1 e) OUZP), pojedinac može od rukovaoca zahtevati *ograničenje obrade podataka* (čl. 18 st. 1 c) OUZP) ukoliko su mu podaci potrebni radi uspostavljanja, ostvarivanja ili odbrane pravnih zahteva.

U pogledu forme, dokaza identiteta, rokova, troškova važe identična pravila kao i za pravo pristupa podacima.

Iako se zahteva da se *podaci bez odlaganja obrišu*, potrebno je od podnošenja zahteva preduzeti adekvatne mere kako bi se podaci obrisali u najkraćem mogućem roku. Takođe moguće je argumentovati i u ovom slučaju da važe opšti rokovi od mesec dana odnosno najduže 3 meseca od podnošenja zahteva (čl. 12 st. 3 OUZP).

Pregled obaveza za rukovaoca po pravu na brisanje podataka „pravu na zaborav“	
Forma	Sve moguće forme (pisana, usmena, elektronska itd.)
Dokaz identiteta	Samo u slučaju sumnje
Rok	Bez odlaganja. Maksimalno 1 mesec od prijema zahteva (najduže 3 meseca po velikom broju zahteva i po kompleksnim zahtevima)

[182] EuGH-Urteil im Fall Rs C-131/12, Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=de&mode=req&dir=&occ=-first&part=1&cid=262486, 09.11.2018.

[183] Gerichtshof der Europäischen Union, Pressemitteilung Nr. 70/14, Luxemburg, den 13. Mai 2014, Urteil in der Rechtssache C-131/12, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, Strana 1, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf, 21.11.2018.

[184] Simone Rosenthal, Felix Bonstein, Wegradiert, *DSGVO – Datenlöschung*, EU- DSGVO konkret, IX Magazin für professionelle Informationsrechnik, 2018., str. 46.

Podaci treba obrisati	✓ Obrada nije neophodna (svrha ispunjena ili otpala) ✓ Povučen pristanak ✓ Uložen prigovor ✓ Nezakonita obrada ✓ Izvršenje pravne obaveze ✓ Podaci dece ✓ Netačni podaci
Zahtev se može odbiti	✓ Sloboda izražavanja i informisanja ✓ Izvršenje pravne obaveze (EU, domaće pravo) ✓ Odbrana pravnih zahteva ✓ Javno zdravlje ✓ Arhiviranje u javnom interesu, naučno istraživanje, statistika
Prava pojedinaca u okviru ostvarivanja prava na brisanje	Pravo na obaveštavanje o korisnicima (samo po zahtevu pojedinaca) ✓ Ako se podaci nezakonito obrađuju, pojedinac može od rukovaoca zahtevati umesto brisanja ograničenje obrade podataka ✓ Ako je pojedinac uložio prigovor, pojedinac može od rukovaoca zahtevati ograničenje obrade podataka ✓ Ako dalja obrada podataka nije potrebna rukovaocu, pojedinac može od rukovaoca zahtevati ograničenje obrade podataka
Obaveza obavešavanja	Svakog korisnika, kome su podaci otkriveni

6.4. Pravo na ograničenje obrade podataka (čl. 18 OUZP)

Pravo na ograničenje podataka predstavlja novo pravo pojedinaca, koje do sada nije postojalo u pravu zaštite podataka. Može se reći da je ovo pravo zapravo propratno pravo pravu na ispravku i pravu na brisanje podataka.

Definicija (čl. 4 tč. 3 OUZP)

„*Ograničavanje obrade*" je obeležavanje uskladištenih podataka o ličnosti u cilju ograničavanja njihove obrade u budućnosti".

Pravo na ograničenje podataka podrazumeva da se *podaci od ostvarivanja ovog prava smeju samo čuvati/snimati*, dok su *ostale radnje obrade isključene* (čl. 4 tč. 2 OUZP).

Ostale radnje obrade su dopuštene (čl. 18 st. 2 OUZP):

- ✓ uz pristanak pojedinaca ili
- ✓ ako su neophodne za uspostavljanje, ostvarivanje ili odbranu pravnih zahteva ili
- ✓ ako su neophodne za zaštitu prava drugog fizičkog ili pravnog lica ili
- ✓ ako su neophodne zbog važnog javnog interesa Unije ili države članice.

Pojedinci mogu da ostvaruju pravo na ograničavanje podataka u sledećim slučajevima:

- ✓ lice na koje se podaci odnose *osporava tačnost podataka* o ličnosti, u roku koji rukovaocu podataka omogućava da proveri tačnost podataka o ličnosti;
- ✓ *obrada je nezakonita*, a lice na koje se podaci odnose se protivi brisanju podataka o ličnosti i umesto toga traži ograničavanje njihove upotrebe;
- ✓ rukovaocu podataka više nisu potrebni podaci o ličnosti za potrebe obrade, ali ih lice na koje se podaci odnose traži radi *uspostavljanja, ostvarivanja ili odbrane pravnih zahteva*;
- ✓ lice na koje se podaci odnose je *uložilo prigovor* na obradu u skladu sa članom 21, stav 1. i još nije potvrđeno da li legitimni razlozi rukovaoca preovlađuju nad razlozima lica na koje se podaci odnose.

Pojedinac koji je ostvario pravo na ograničenje obrade mora biti od rukovaoca *obavešten pre ukidanja ograničenja obrade* (čl. 18 st. 3 OUZP).

U pogledu forme, dokaza identiteta, rokova, troškova važe identična pravila kao i za pravo pristupa podacima.

Rukovalac je u obavezi da *informiše svakog primaoca o ograničenju podataka* (čl. 19 OUZP), kome su podaci otkriveni. Jedini izuzetak bi bio kada je to nemoguće ili kada je nesrazmerno komplikovano.[185] *Pravo na obaveštavanje pojedinca o tim korisnicima* je moguće *na zahtev pogođenih pojedinaca* (čl. 19 OUZP).

Pregled obaveza za rukovaoca po pravu na ograničenje obrade podataka	
Forma	Sve moguće forme (pisana, usmena, elektronska itd.)
Dokaz identiteta	Samo u slučaju sumnje
Rok	Maksimalno 1 mesec od prijema zahteva (najduže 3 meseca po velikom broju zahteva i po kompleksnim zahtevima)
Podatke treba ograničiti na zahtev pojedinca	✓ Osporena tačnost podataka ✓ Nezakonita obrada ✓ Obrada nije neophodna rukovaocu ✓ Uložen prigovor

[185] *Ibidem*, str. 133.

Odobren zahtev proizvodi dejstva	Podaci se smeju samo čuvati/snimati Ostale radnje obrade: ✓ Samo uz pristanak pojedinca ✓ Ako je obrada neophodna za uspostavljanje, ostvarivanje ili odbranu pravnih zahteva ✓ Ako je obrada neophodna za zaštitu prava drugog fizičkog ili pravnog lica ✓ Ako je obrada neophodna zbog važnog javnog interesa Unije ili države članice
Prava pojedinaca u okviru ostvarivanja prava na brisanje	Pravo na obaveštavanje o korisnicima (samo po zahtevu pojedinaca) ✓ Ako se podaci nezakonito obrađuju, pojedinac može od rukovaoca zahtevati umesto brisanja ograničenje obrade podataka ✓ Ako je pojedinac uložio prigovor, pojedinac može od rukovaoca zahtevati ograničenje obrade podataka ✓ Ako dalja obrada podataka nije potrebna rukovaocu, pojedinac može od rukovaoca zahtevati ograničenje obrade podataka
Obaveza obavešavanja	Svakog korisnika, kome su podaci otkriveni

6.5. Pravo na prenosivost podataka (čl. 20 OUZP)

Donošenjem OUZP uvodi se novo pravo pojedinaca, koje je usko povezano sa pravom pristupa (čl. 15 OUZP), a to je pravo na prenosivost podataka. Ovo pravo se značajno razlikuje od prava pristupa. Njime se pojedincima omogućava da dobiju tj. pristupe podacima o ličnosti koje rukovalac o njima obrađuje u strukturisanom, uobičajeno upotrebljavanom i mašinski čitljivom formatu kao i da prenesu te podatke drugom rukovaocu. Ovo pravo ima za cilj da omogući *pojedincima veću kontrolu nad podacima* o ličnosti i osnaži njihova prava. Prenosivost podataka predstavlja na taj način mogućnost uspostavljanja ravnoteže između pojedinaca i rukovaoca.

Osim toga ovo pravo ima za cilj da podstakne *takmičenje na tržištu,* pošto se njime omogućava direktan prenos od jednog do drugog rukovaoca. Uz to menjanje pružaoca usluga utiče i na razvoj novih usluga na digitalnom tržištu. Ovim pravom obezbeđuje se bolja pozicija potrošača zbog *sprečavanja zavisnosti od dobavljača*. Pored toga ovo pravo treba da omogući nove šanse *za inovacije* i razmenu podataka o ličnosti između rukovaoca na bezbedan način.

Pravo na prenosivost definisano je na sledeći način (čl. 20 st. 1 OUZP): "Lice na koje se podaci odnose ima pravo da primi podatke o ličnosti koji se odnose na njega, a koje je pružilo rukovaocu podataka u strukturiranom, uobičajenom i mašinski čitljivom formatu i ima pravo da prenosi te podatke drugom rukovaocu podataka bez ometanja od strane rukovaoca kojem su podaci o ličnosti pruženi…".

Prenosivost podataka je pravo pojedinca na *primanje dela evidencije podataka o ličnosti,* koju o njemu obrađuje rukovalac. Pravo pojedinca na primanje dela evidencije podataka o ličnosti odnosi se i na *primanje ovih podataka za dalju ličnu upotrebu*. Pojedinac bi trebalo da svoje podatke o ličnosti dobije tako što će mu ih rukovalac ili *snimiti na privatni prenosni medijum* (npr. USB, CD) ili *preko tehnologija koja omogućava korišćenje različitih informatičkih usluga na fizički udaljenim serverima* (private cloud) bez potrebe za prenosom podataka drugom rukovaocu. Ovime se pojedincima omogućava da na jednostavan način sami upravljaju podacima o ličnosti i da ih dalje koriste po potrebi.

Podaci koji se primaju treba da budu u „strukturisanom, uobičajeno upotrebljavanom i mašinski čitljivom formatu".

PRIMERI
Pojedinac želi da preuzme listu svojih kontakata iz aplikacije za mejl poštu, kako bi sastavio listu zvanica za venčanje. Pojedinac želi da se informiše o kupovinama u kojima je koristio razne članske kartice, da bi procenio svoju potrošnju u supermarketima.

Pored prava na primanje podataka o ličnosti, pojedincima treba obezbediti i *pravo prenosa podataka o ličnosti od jednog rukovaoca do drugog bez ometanja* (čl. 20 st. 1 OUZP). Ovim elementom prenosivosti podataka pojedincima se omogućava ne samo da prime podatke i da ih ponovno upotrebe, nego i da podatke prenesu drugom rukovaocu (u istoj ili nekoj drugoj branši).

Na zahtev pojedinca i *ako je to tehnički izvodljivo* podaci se mogu preneti *neposredno od jednog rukovaoca do drugog* (čl. 20 st. 2 OUZP). U tom smislu se rukovalac podstiče da razvija interoperabilne formate koji bi omogućili prenosivost podataka između rukovaoca i drugih rukovaoca (U.t.r. 68 OUZP). Sa druge strane rukovalac nije u obavezi da upotrebljava ili održava tehnički kompatibilne sisteme za obradu podataka, pa je stoga poželjno da se izrade takvi formati koji bi omogućili jednostavan pristup pojedincima ili rukovaocima.

Pravo na prenosivost podataka omogućava pojedincima da svoje podatke prime i obrađuju *u skladu sa sopstvenim željama.* U tom smislu je rukovalac dužan da odgovori na zahteve pojedinaca za prenos. *Rukovalac svakako nije odgovoran* za obradu podataka pojedinca ili drugih rukovaoca koji će podatke primiti. Prilikom sprovođenja ovog prava rukovaoci deluju u ime pojedinaca, pa ih stoga *rukovaoce možemo smatrati kao obrađivače odnosno pružaoce servisa prenosa podataka*. Rukovalac nije odgovoran za usklađenost rukovaoca koji prima podatake sa OUZP, pošto rukovalac koji šalje podatke ne odlučuje o izboru primaoca podataka.

Rukovalac treba da preduzme adekvatne mere, da bi mogao da deluje u ime pojedinca. To se pre svega odnosi na *procese* u kojima bi se obezbedilo da se prenese vrsta podataka koju pojedinac želi da prenese. Adekvatne mere zaštite bi bile: potvrda pojedinca pre prenosa ili saglasnost pojedinca za prenos ili regulisanje prilikom sklapanja ugovora.

U odgovoru na zahtev pojedinaca i pre prenosa podataka rukovaoci nisu odgovorni da proveravaju kvalitet podataka. Predpostavlja se naravno da su podaci tačni i ažurirani (shodno načelu tačnosti zaštite podataka iz čl. 5 st. 1 d) OUZP). Pored toga rukovaoci nemaju obavezu dužeg čuvanja podataka koji se prenose drugim rukovaocima nego što je potrebno ili nakon isteka perioda čuvanja. Ne postoji dakle opravdanje ili dopuštenost dalje obrade podataka (izuzev zakonskih obaveza čuvanja) da bi se npr. ubuduće udovoljilo zahtevima za prenos podataka.

U slučaju da podatke zahtevane za prenos obrađuje obrađivač, *obrađivač je u obavezi da pomogne rukovaocu*. Obavezu pomaganja obrađivača *treba regulisati ugovorom* (čl. 28 OUZP) kao jednu od tehničko organizacionih mera u svrhu odgovora na zahteve pojedinaca.

Kada se radi o *zajedničkim rukovaocima* takođe treba *ugovorom jasno rasporediti dužnosti* između svih rukovaoca u pogledu obrade zahteva pojedinaca za prenosivost podataka.

Sa druge strane *rukovalac koji prima podatke* treba da obezbedi da su *podaci koje prima relevantni i da nisu prekomerni*. To bi u praksi značilo da ukoliko rukovalac prosledi nepotrebne podatke za drugog rukovaoca i koji nisu neophodni za obradu u svrhe drugog rukovaoca ("novi rukovalac"), novi rukovalac je dužan da te podatke obriše.

Prijemom podataka organizacija koja podatke prima postaje *nov rukovalac* i stoga mora poštovati načela obrade podataka (čl. 5 OUZP). U pogledu ove druge obrade podataka, smatra se da je *podatke pružio sam pojedinac*, pa se stoga može govoriti o *novoj obradi*. Ne radi se dakle o obradi u različite svrhe u odnosu na prvobitnu od strane istog rukovaoca (čl. 6 st. 4 OUZP), već o potpuno novoj obradi podataka.

Rukovaoci koji bi trebalo da prime podatke (potencijalni novi rukovaoci), mogu *da prime podatke* pojedinaca, ali *nisu u obavezi da to učine*. Obaveza da omogući prenostivost tiče se rukovaoca.[186]

Samo ostvarivanje prava na prenosivost podataka *ne dovodi u pitanje bilo koje drugo pravo pojedinca*. Tako pojedinac može da nastavi da koristi usluge rukovaoca i nakon sprovedenog postupka prenosa podataka. Sam postupak prenosa podataka *ne pokreće automatski brisanje podataka pojedinca i ne utiče na period čuvanja podataka*. Zbog toga pojedinac može i dalje da ostvaruje svoja prava, pošto *rukovalac i dalje obrađuje podatke o njemu*. U slučaju da pojedinac podnese zahtev za brisanje podataka (čl. 17 OUZP), rukovalac ne sme da taj zahtev odbije ili odloži sa obrazloženjem vezanim za prenos podataka (čl. 20 st. 3 OUZP).

[186] Radna grupa član 29, Die Datenschutzgruppe Artikel 29, *Smernice o pravu na prenosivost podataka*, Leitlinien zum Recht auf Datenübertragbarkeit, usvojeno 13. decembra 2016, revidirano 05.04.2017., 16/DE, WP 242 rev.01, str. 3, 4, 5, 6, 7.

Rukovaoci su u obavezi da obezbede *zakonitost obrade podataka*, pa stoga moraju da imaju jasno definisanu pravnu osnovu obrade podataka. *Da bi uopšte došlo do primene prava prenosivosti podataka*, podrazumeva se da rukovalac obrađuje podatke po sledećim pravnim osnovama (čl. 20 st. 1 a) OUZP):

- ✓ *pristanak* pojedinca (u skladu sa čl. 6 st. 1 a) OUZP ili u skladu sa čl. 9 st. 2 a) OUZP ako su u pitanju posebne kategorije podataka o ličnosti), ili
- ✓ *ugovor* u kojem je pojedinac stranka (u skladu sa čl. 6 st. 1 b) OUZP).

PRIMER UGOVOR KAO PRAVNI OSNOV
Knjige koje je pojedinac kupio preko interneta ili pesme koje je slušao u okviru neke onlajn usluge baziraju se na izvršavanju ugovora u kojem je pojedinac jedna od ugovornih strana. Stoga ove situacije spadaju u područje primene prenosivosti podataka.

Treba napomenuti da se pravo prenosivosti podataka ne odnosi na ostale slučajeve dopuštenosti obrade podataka! To znači da se *pravo prenosivosti ne odnosi* na one obrade podataka koji za pravni osnov imaju *pravnu obavezu, pretežnije interese, životne interese pojedinaca, javni interes kao i ostale uslove dopuštenosti obrade posebnih kategorija podataka iz čl. 9 st. 2 OUZP (izuzev čl. 9 st. 2 a) OUZP)*.

PRIMER PRAVNA OBAVEZA KAO PRAVNI OSNOV
Finansijske institucije nisu u obavezi da odgovore na zahtev za prenosivost podataka koji se odnosi na podatke o ličnosti, koji se obrađuju kao *deo njihove zakonske obaveze* sprečavanja i otkrivanja pranja novca i drugih finansijskih krivičnih dela.

PRIMER UGOVOR PRAVNA LICA KAO PRAVNI OSNOV
Prenosivost podataka se ne primenjuje i situacijama vezanim za poslovne kontakt podatke, koji se obrađuju u okviru odnosa između poslovnih subjekata, ukoliko se obrada ne bazira na pristanku ili na ugovoru u kojem je ugovorna strana pojedinac.

PRIMER RADNOPRAVNI ODNOSI
Kada se radi o podacima o zaposlenima, pravo na prenosivost podataka se primjenjuje *samo ako se obrada bazira na ugovoru* u kome je pojedinac stranka u ugovoru. Takođe to važi i za situacije u kojima se *pristanak* pojavljuje kao pravni osnov (npr. rođendanske liste, fotografije). Postoje i obrade podataka u radnom okruženju koje se temelje na pravnoj osnovi pretežnijeg interesa ili koje su nužne radi ispunjivanja određenih pravnih obaveza u području zapošljavanja. Pravo na prenosivost podataka se odnosi na situacije kao što su npr. isplate zarada i isplate naknada, interno zapošljavanje. U većini slučajeva neophodno je proceniti da li su ispunjenji svi uslovi da bi došlo do primene prava na prenosivost podataka.

Pravo na prenosivost podataka primjenjuje se samo ako se obrada podataka „sprovodi *automatskim putem*". To znači da *za obradu podataka u papirnom formatu pravo prenosivosti podataka nije primenljivo*.

Da bi došlo do primene prava na prenosivost podataka (čl. 20 st. 1 OUZP) podaci moraju biti:

- ✓ *lični* tj. da se odnose na pojedinca i
- ✓ podaci koje je pojedinac *pružio* rukovaocu
- ✓ ostvarivanje prava na prenosivost podataka *ne sme negativno da utiče na prava i slobode drugih* (čl. 20 st. 4 OUZP).

Primena zahteva za prenosivost podataka odnosi se *samo na podatke o ličnosti*. Anonimni podaci i oni koji se ne odnose na pojedinca ne primenjuju se na ovo pravo. Sa druge strane doći će do primene prava prenosivosti podataka kod podataka koji su pseudonimizovani i na osnovu kojih se može jasno identifikovati određeni pojedinac (npr. ako pojedinac pruži odgovarajuće identifikacione elemente shodno čl 11 st. 2 OUZP). U mnogim situacijama će rukovalac obrađivati podatke, koji se odnose podatke o ličnosti od više lica. Tada rukovalac ne treba da usko tumači odredbu „podaci o ličnosti, koji se odnose na pojedinca".

Primena zahteva za prenosivost podataka odnosi se samo na one situacije, *kada je podatke pružio pojedinac.* Pritom je od značaja da je pojedinac ove podatke *svesno i aktivno pružio* (npr. poštanska adresa, korisničko ime, godine dostavljeni putem internet obrazaca).

Naročito u novije vreme (npr. uz pomoć BIG DATA alata) postoje mnogobrojni podaci koje pojedinac pruža, a koje potiču od posmatranja njegovih aktivnosti. Radna grupa član 29 smatra da bi radi potpunog ostvarivanja ovog prava rukovaoci trebalo da uključe i *podatke o ličnosti koji su zabeleženi na osnovu aktivnosti korisnika* (npr. "sirovi podaci" koji se obrađuju kod pametnog merenja, podaci o lokaciji, podaci dobijeni iz međusobno povezanih uređaja, samovozećih automobila, pametnih stvari, istorijat pretraživanja i korišćenja internet stranica).

Podaci na osnovu kojih *rukovalac sam zaključuje i izvodi procene ne dovode do primene prava prenosivosti*.

PRIMER
Procena rizika koja se odnosi na stanje korisnika ili profila i finansijskih propisa (npr. radi ocene kreditne sposobnosti ili usklađivanja sa pravilima protiv pranja novca). Iako takvi podaci mogu biti deo profila iz kojih se zaključuje ili izvodi na osnovu analize podataka koje je pružio pojedinac (npr. putem svojih aktivnosti), obično se neće smatrati da je te podatke pružio pojedinac, pa stoga neće biti obuhvaćeni pravom prenosivosti podataka.

Podaci na osnovu aktivnosti pojedinaca, koje rukovalac obrađuje, *a koji su izvedeni iz analize ili se izvode iz ovih aktivnosti, potpadaju pod podatke koje pojedinac pruža*. Stoga se na iste primenjuje pravo prenosivosti (npr. rezultati algoritma neke aplikacije). Samo podaci izvedeni iz zaključaka ili izvedeni podaci ne potpadaju pod pravo prenosivosti podataka. To su podaci i *rezultati do kojih je rukovalac sam došao*.[187]

[187] *Ibidem*, str. 8, 10, 11, 12.

Kada se radi o podacima o ličnosti koji se odnose na druge pojedince, ovaj uslov onemogućava novog rukovaoca da pronalazi i prenosi podatke koji sadrže podatke o drugim pojedincima (bez njihovog pristanka) u situacijama kada je verovatno da će se ti podaci obrađivati na način koji *negativno utiče na prava i slobode drugih pojedinaca* (čl. 20 st. 4 OUZP). U U.t.r. 68 OUZP navodi se da "ako se određeni skup podataka o ličnosti odnosi na više lica na koje se podaci odnose, pravo na primanje tih podataka o ličnosti ne sme da dovodi u pitanje prava i sloboda ostalih lice na koje se podaci odnose u skladu s ovom uredbom".

PRIMERI
Negativan uticaj na druge pojedince bi postojao, ako bi prenosom podataka drugi pojedinci bili sprečeni u ostvarivanju prava shodno OUZP (npr. pravo na informisanje, pravo na pristup itd). Bankovni račun pojedinca može da sadrži i podatke o ličnosti koji se odnose na transakcije lica koje je podnelo zahtev, ali i druge pojedinaca (npr. slanje novca vlasniku računa). U ovom slučaju nije verovatno da će prenos podataka o bankovnom računu vlasniku računa negativno uticati na prava i slobode drugih pojedinaca. Preduslov za ovo je da se podaci upotrebljavaju u istu svrhu (npr. adresa za kontakt koju upotrebljava samo pojedinac podnosilac zahteva ili istorija bankovnog računa pojedinca podnosoca zahteva).

Prava drugih mogu biti povređena ukoliko se radi o *poslovnim tajnama* ili intelektualnoj svojini odnosno *autorskim pravima* (pre svega kada su u pitanju zaštićeni softverski programi). Ova prava svakako ne smeju da utiču na taj način da u potpunosti onemoguće ostvarivanje prava pojedinaca kao i da dovedu generalno do odbijanja pružanja informacija pojedincu. Rukovalac ne sme da odbije zahtev za prenosivost podataka ako je prekršeno neko ugovorno pravo drugih pojedincaca (npr. nepružena usluga, neplaćen dug itd).

U pogledu pružanja informacija pojedincima kada bi moglo doći do kršenja poslovne tajne ili povrede intelektualne svojine rukovaoci treba da obrate pažnju da ove informacije ne otkriju pojedincima. *Sam rizik po otkrivanje ovih informacija ne može biti osnova za odbijanje* zahteva pojedinaca.[188]

Pojedinci imaju pravo da *bez ometanja prenose podatke drugom rukovaocu* (čl. 20 st. 1 OUZP). Ometanje prema mišljenju Radne grupe član 29 može biti svaka pravna, tehnička ili financijska prepreka kojom rukovalac zaustavlja ili usporava pristup, prenos ili ponovnu upotrebu podataka pojedinaca ili drugog rukovaoca.

PRIMERI OMETANJA
Naknade koje se traže za dostavljanje podataka, nedostatak interoperabilnosti ili pristupa određenom formatu podataka, prekomerno odlaganje ili komplikovani postupak pronalaženja podataka, namerno sakrivanje podataka ili posebni, neprimereni ili neopravdani sektorski zahtevi u pogledu normizacije ili akreditacije.

[188] *Ibidem*, str. 13, 15, 16, 17.

Rukovaoci treba da omoguće *direktan prenos podataka drugim rukovaocima ako je to tehnički izvodljivo* (čl. 20 st. 2 OUZP). Tehničku izvodljivost prenosa treba procenjivati od slučaja do slučaja, a ovaj zahtev „ne treba da obavezuje rukovaoca da koristi ili održava tehnički kompatibilne sisteme za obradu“ (U.t.r. 68 OUZP).

Rukovalac je pre svega u obavezi da obezbedi da se podaci mogu preneti u interoperabilnom formatu. Međutim treba imati u vidu, da se ovime ne nameće obaveza drugim rukovaocima da podrže te formate. Na taj način bi direktan prenos bio moguć od jednog rukovaoca do drugog samo u slučaju *bezbedne komunikacije između dva sistema* (rukovaoca pošiljalaca i rukovaoca primaoca). To podrazumeva mogućnost odgovarajuće međusobne identifikacije sistema kao i korišćenje metoda kriptografije.

U slučaju da direktan prenos nije moguć iz tehničkih razloga, rukovalac treba da o ovome informiše pojedince prilikom odgovora na zahtev. Ukoliko to ne učini rukovalac rizikuje pravnu kvalifikaciju „odbijanja zahteva“, što dovodi do mogućnosti podnošenja žalbe nadzornom organu ili korišćenja drugih pravnih lekova (čl. 12 st. 4 OUZP).

Rukovaoci su u obavezi da podatke pruže u *odgovarajućem formatu*, tako da pojedinci ponovo mogu da ih koriste (čl. 20 st. 1 OUZP). Podaci moraju da budu pruženi *u strukturiranom, uobičajenom i* mašinski *čitljivom formatu*. Taj format trebalo da bude *interoperabilan*, što označava “sposobnost interakcije različitih i raznovrsnih organizacija sa obostrano korisnim i dogovorenim zajedničkim ciljevima, *uključujući razmenu informacija i znanja između organizacija, putem poslovnih procesa koje podržavaju, razmenjujući podatke između svojih IKT sistema*”.[189]

Pojmovi „*strukturisan*”, „*uobičajen*” i „*mašinski čitljiv*” predstavljaju minimalne standarde za interoperabilnost formata podataka koje treba rukovalac da pruži. Pojam „*mašinski čitljiv dokument*” (U.t.r. 21 Direktive 2013/37/EU o ponovnoj upotrebi informacija javnog sektora) je definisan kao: „oblik datoteke strukturisan tako da se programske aplikacije mogu lako identifikovati, prepoznati i iz nje izvaditi specifične podatke, uključujući pojedinačna obaveštenja i njihovu unutrašnju strukturu. Podaci šifrovani u datotekama koji su strukturisani u mašinski čitljivom formatu jesu mašinski čitljivi podaci. Mašinski čitljivi formati mogu biti otvoreni ili zaštićeni; mogu biti u formalnom standardu ili ne. Za šifrovane dokumente u obliku datoteke koja ograničava automatsku obradu, pošto se podaci ili ne mogu, ili ne mogu lako, iz nje izvaditi, ne bi se trebalo smatrati da su u mašinski čitljivom formatu. Države članice bi trebalo da podstiču upotrebu otvorenih, mašinski čitljivih formata“.

U U.t.r 68 OUZP razjašnjena je obaveza rukovaoca „pravo lica na koje se podaci odnose na prenos ili primanje podataka o ličnosti koji se odnose na njega ne treba da obavezuje rukovaoca da koristi ili održava tehnički kompatibilne sisteme za obradu”. Pravo prenosivosti podataka treba dakle da *omogući interoperabilne sisteme, a ne kompatibilne sisteme*.

---

[189] Član 2. Odluke br. 922/2009/EZ Evropskog parlamenta i Veća od 16. septembra 2009. o interoperabilnim rešenjima za evropske javne uprave (ISA) (SL L 260, 03.10.2009., str. 20.

Ubičajeni otvoreni formati su npr. *XML, JSON, CSV* zajedno sa korisnim *metapodacima* na najvišem mogućem nivou detalja, istovremenono održavajući visok nivo apstrakcije. Podatke o porukama e-pošte trebalo bi pružati u formatu koji zadržava sve metapodatke kako bi se omogućila ponovna upotreba podataka. U slučaju da rukovalac omogući izbor pojedincu u pogledu željenog formata trebalo bi detaljno da objasi posledice tog izbora.

OUZP ne daje odgovor na pitanje, kako postupiti u slučaju obimniih ili kompleksnih obrada podataka o ličnosti. Prema mišljenju Radne grupe član 29 najvažnije da pojedinac bude u poziciji u kojoj može u potpunosti da shvati definiciju, raspored i strukturu podataka o ličnosti koje mu pruža rukovalac.

Bezbednost podataka je jedno od načela zaštite podataka (čl. 5 st. 1 f) OUZP). Stoga rukovaoci generalno treba da obezbede bezbedonosne standarde. Sam prenos podataka o ličnosti pojedincu predstavlja veliki izazov za bezbednost podataka. Uzimajući u obzir da je cilj prenosivosti dobijanje podataka o ličnosti iz informacionih sistema rukovaoca, prenos može biti *rizičan iz razloga povreda bezbednosi podataka o ličnosti*. Pošto je rukovalac odgovoran za preduzimanje odgovarajućih tehničkih i organizacionih mera, trebalo bi da uzme u obzir kod prenosa podataka adekvatne *kriptografske metode* do odgovarajućeg odredišta uz pomoć primene adekvatnih mera *autentifikacije*. Rukovaoci bi trebalo da procene konkretne rizike prenosa podataka i da preduzmu adekvatne mere za njihovo umanjenje. Implementacija odgovarajućih mera zaštite važi i za podatke o ličnosti koji ostaju u njegovom sistemu kao i za postupak rešavanja problema u slučaju povreda bezbednosti podataka. Mere za umanjenje rizika mogu biti: ako je potrebno identifikovati pojedinca, upotreba dodatnih informacija za autentifikaciju kao što su zajednička tajna (eng. shared secret) ili neki drugi način autentifikacije kao što je jednokratna šifra; zaustavljanje ili blokiranje transakcije odnosno prenosa podataka ako postoji sumnja da je račun kompromitovan. U slučajevima direktnog prenosa drugom rukovaocu trebalo bi upotrebljavati autentifikaciju uz odobrenje kao što je autentifikacija na temelju tokena.[190]

Pojedinci kojima se prenose podaci mogu preneti podatke na sopstvene sisteme koji su manje bezbedni od onih koje nudi rukovalac. Kao što je istaknuto rukovalac nije odgovoran za to na koji nacin će podaci biti obrađivani, čuvani i koji stepen bezbednosti će biti implementiran kod pojedinaca ili drugih (novih) rukovaoca. Rukovalac bi trebalo da pojedinca obavesti o tome, kako da zaštiti bezbednost svojih podataka koje je primio. Rukovalac može to učiniti putem preporuke odgovarajućeg formata, kriptografske metode ili alata i drugih zaštitnih mera koje bi bile od pomoći u odnosu na određenu situaciju.[191]

U pogledu forme, dokaza identiteta, rokova, troškova važe identična pravila kao i za pravo pristupa podacima.

---

[190] "Token" je hardverski uređaj ili softversko rešenje zasnovano n akriptografiji, koje omogućava naprednu autentifikaciju u realnom vremenu.

[191] Radna grupa član 29, Die Datenschutzgruppe Artikel 29, *Smernice o pravu na prenosivost podataka*, Leitlinien zum Recht auf Datenübertragbarkeit, usvojeno 13. decembra 2016, revidirano 05.04.2017., 16/DE, WP 242 rev.01, str. 18, 19, 20, 21, 22, 23.

Pregled obaveza za rukovaoca po pravu na prenosivost podataka	
Forma	Sve moguće forme (pisana, usmena, elektronska itd.)
Dokaz identiteta	Samo u slučaju sumnje
Rok	Maksimalno 1 mesec od prijema zahteva (najduže 3 meseca po velikom broju zahteva i po kompleksnim zahtevima)
Zakonska dopuštenost ostvarivanja prava na prenosivost podataka	✓ pristanak ✓ ugovor ✓ automatska obrada podataka
Format prenosivih podataka	✓ strukturisan ✓ uobičajen ✓ mašinski čitljiv
Odbijanje zahteva	✓ Ne radi se o ličnim podacima pojedinaca ✓ Podatke nije pružio direktno pojedinac ✓ Prenos utiče na prava i slobode drugih
Ostala prava pojedinaca	Direktan prenos između rukovaoca ako je to tehnički moguće

6.6. Pravo na prigovor (čl. 21 OUZP)

Pravo prigovora je dopušteno u određenim situacijama:

- ✓ Kada se podaci obrađuju radi izvršenje zadatka koji se obavlja u *javnom interesu* ili u okviru izvršavanja službenih ovlašćenja dodeljenih rukovaocu (čl. 6 st. 1 e) OUZP) *uključujući profilisanje* zasnovano na ovom pravnom osnovu, ili
- ✓ Kada se podaci obrađuju zbog *legitimnih (pretežnijih) interesa rukovaova ili trećeg lica* (čl. 6 st. 1 f) OUZP), ili
- ✓ Kada se podaci obrađuju za potrebe *direktnog marketinga i profilisanja*, ako je povezano sa takvim direktnim marketingom (čl. 21 st. 2 OUZP), ili
- ✓ U kontekstu korišćenja *usluga informacionog društva* (čl. 21 st. 5 OUZP), ili
- ✓ Ako se podaci o ličnosti obrađuju u svrhe *naučnog ili istorijskog istraživanja ili u statističke svrhe* (čl. 21 st. 6 OUZP).

Prigovor po osnovu javnog interesa i legitimnih interesa

Za tačke 1 i 2 (čl. 21 st. 1 OUZP) važi to da rukovalac *ne sme više da obrađuje podatke po uloženom prigovoru pojedinca*. To bi u praksi značilo da te *podatke mora da obriše* (čl. 17 st. 1 c) OUZP), za razliku od ograničavanja obrade podataka (gde postoji radnja obrade u vidu čuvanja)! Na taj način zapravo *pravo na prigovor prelazi u pravo na brisanje podataka* iz čl. 17 OUZP. *Pravo na brisanje nije neophodno zahtevati posebno*!

Izuzetak (čl. 21 st. 1 OUZP) od ostvarivanja prava po uloženom prigovoru *za tačke 1 i 2* postoji:

- ✓ ako je *rukovalac* u stanju da *dokaže da postoje uverljivi legitimni razlozi za obradu koji preovlađuju* nad interesima, pravima i slobodama pojedinaca, ili
- ✓ ako su podaci neophodni *radi uspostavljanja, ostvarivanja ili odbrane pravnih zahteva.*

Najkasnije prilikom prve komunikacije treba *ukazati pojedincu na pravo prigovora* iz tačke 1 i 2 i to *jasno i odvojeno od svih drugih informacija* (čl. 21 st. 4 OUZP).

Po uloženom prigovoru pojedinac ima pravo da *zahteva ograničavanje obrade*, ako još *nije potvrđeno da li legitimni razlozi rukovaoca preovlađuju nad razlozima lica* na koje se podaci odnose (čl. 18 st. 1 d) OUZP). Na taj način pored prava prigovora u toku same obrade zahteva *postoji i pravo na ograničavanje obrade*.

Prigovor po osnovu direktnog marketinga i profilisanja

Za razliku od tački 1 i 2, prigovor po *tački 3* ima apsolutno dejstvo. To znači da se prigovor po osnovu direktnog marketinga (što može da uključi i profilisanje) može *u bilo kom trenutku uložiti i bez ograničenja primeniti* (čl. 21 st. 2 OUZP).

Ukoliko pojedinac uloži prigovor po ovom osnovu, rukovalac *ne sme više da obrađuje podatke po uloženom prigovoru pojedinca* (čl. 21 st. 3 OUZP). To bi u praksi značilo da te *podatke mora da obriše* (čl. 17 st. 1 c) OUZP), za razliku od ograničavanja obrade podataka (gde postoji radnja obrade u vidu čuvanja)! Na taj način zapravo *pravo na prigovor prelazi u pravo na brisanje podataka* iz čl. 17 OUZP. *Pravo na brisanje nije neophodno zahtevati posebno*!

Prigovor u kontekstu korišćenja usluga informacionog društva

Pojedinac po uloženom prigovoru po *tački 4* treba da bude u mogućnosti da svoje pravo ostvari *automatskim putem pomoću tehničkih specifikacija* (čl. 21 st. 5 OUZP). To bi značilo da u softversko rešenje treba da bude ugrađen mehanizam za odbijanje podataka (npr. odbijanje kolačića na veb stranicama). Na ovom mestu treba istaći da OUZP nije regulisao, šta se dešava sa podacima po uloženom prigovoru po ovom osnovu. Naime čl. 17 st. 1 f) OUZP predviđa brisanje podataka, u slučaju da se radi o podacima dece u vezi sa uslugama informacionog društva (iz čl. 8 st. 1 OUZP). Stoga ostaje *sporno na koje usluge informacionog društva je zakonodavac* tačno mislio vezano za pravo prigovora u ovom slučaju. Ne ulazeći u dalje teoretisanje ovog problema, suština je da za podatke dece postoji pravo na brisanje podataka po osnovu čl. 17 st. 1 f) OUZP, koje posebno može biti zahtevano. Činjenica je da pravo prigovora po ovom osnovu samo bez zahteva za brisanje ne dovodi do automatskog brisanja podataka, pre bi se moglo reći da dolazi do *neke vrste ograničenja obrade podataka*.

Prigovor u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe

Izuzetak (čl. 21 st. 6 OUZP) od ostvarivanja prava po uloženom prigovoru *za tačku 5* postoji u slučaju ako je *obrada neophodna za izvršenje zadatka koji se obavlja u javnom interesu*.

I u ovom slučaju OUZP nije regulisao pravna dejstva po uloženom prigovoru. Tako da nije poznato šta će se desiti sa podacima, da li se oni moraju čuvati ili ograničiti njihova obrada ili se trebaju obrisati.[192]

[192] Viktoria Haidinger, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 135.

7. PRIVACY BY DESIGN I PRIVACY BY DEFAULT (čl. 25 OUZP)

7.1. Privacy by design

Princip Privacy by Design nastao je devedesetih godina dvadesetog veka. Zaslužna za proklamovanje ovog principa je En Čavoukian tadašnja kanadska poverenica za slobodu informacija i zaštitu podataka pokrajine Otava.

Privacy by Design se sastoji od 7 suštinskih elementa:

1. Proaktivnost, a ne reaktivnost; prevencija a ne korekcija;
2. Zaštita podataka po difoltu odnosno podrazumevana zaštita podataka („Privacy by Default“);
3. Zaštita podataka integrisana u dizajn;
4. Potpuna funkcionalnost – pozitivna suma, a ne negativna suma;
5. Potpuna bezbednost – zaštita tokom čitavog životnog ciklusa;
6. Vidljivost i transparentnost – voditi računa o otvorenost;
7. Zaštita privatnosti korisnika – voditi računa o tome da korisnik bude u fokusu.

Ovim principom nastoji se da budu ispoštovana pravila zaštite podataka još od najranije faze projekta i da se deluje proaktivno i preventivno u smislu zaštitie prava pojedinaca. Na taj način princip Privacy by Design ima identičnu proaktivnu ulogu kao i procena uticaja u vezi sa zaštitom podataka (čl. 35 OUZP). Poštovanje ovog principa se pre svega zahteva od strane kreatora i lica zaduženih za tehnički razvoj sistema.

Iako je ovaj princip od svog samog starta kritikovan zbog svoje apstraktnosti i primenljivosti u praksi, postoje neke smernice u praksi, kojima bi rukovaoci, ali i obrađivači trebalo da se vode:

- ✓ Minimizacija: Količinu ličnih podataka, koji se obrađuju treba smanjiti na najmanju moguću meru,
- ✓ Sakrivanje: Podatke o ličnosti i njihove veze treba, ako je to moguće maskirati i sakrivati,
- ✓ Odvajanje: Podatke o ličnosti treba, ako je to moguće, odvojeno obrađivati i odvojeno snimati/čuvati,
- ✓ Objedinjavanje: Podatke o ličnosti treba na najvišem nivou objediniti i na najnižem nivou detalja obrađivati, a da oni ispune svoju svrhu,
- ✓ Informisanost: Pojedince treba proporcionalno obaveštavati, ukoliko se obrađuju njihovi podaci o ličnosti,
- ✓ Kontrola: Pojedinci treba da zadrže kontrolu o podacima koji se ne njih odnose u postupku obrade,

- ✓ Sprovođenje: Pravni zahtevi treba da budu u skladu sa pravilima o zaštiti podataka i da budu sprovodivi,
- ✓ Proveljivost: Rukovaoci treba da budu u stanju da dokažu pridržavanje pravila zaštite podataka i svih zakonskih odredbi.

Prva četri elementa se odnose na tehničko postupanje u vezi sa podacima, dok su ostala četri elementa procesno orijentisana, i oni se odnose na uopštene zahteve iz prava zaštite podataka.[193]

OUZP je principe Privacy by Design i Privacy by Default regulisao u svom čl. 25. Sam naslov ovog člana „*Ugrađena i podrazumevana zaštita podataka*" ukazuje da se radi o 2 principa, iako je u nacrtu OUZP bila drugačija formulacija „zaštita podataka putem tehnike". Kao što se može iz elemenata Privacy by Design zaključiti, Privacy by Default bi bio deo koncepta Privacy by Design.

Privacy by Default znači da su postavke nekog sistema podrazumevane i napravljene tako da unapred štite podatke o ličnosti, kada određeni pojedinac želi da koristi neki proizvod ili uslugu. Shodno ovom principu trebalo bi da podešavanja budu deaktivirana, ali da se po potrebi mogu aktivirati. Na taj način se kombinuju korisnička jednostavnost u smislu zaštite podataka i fleksibilnost.

Čl. 25 st. 1 OUZP definiše princip Privacy by Design: „Uzimajući u obzir najnoviji tehnološki razvoj, troškove sprovođenja i prirodu, obim, kontekst i svrhe obrade, kao i rizike različitih stepena verovatnoće i ozbiljnosti za prava i slobode fizičkih lica koji proizilaze iz obrade podataka, rukovalac *prilikom određivanja sredstava obrade i prilikom same obrade* primenjuje odgovarajuće tehničke i organizacione mere, poput pseudonimizacije, koje su osmišljene za delotvorno *sprovođenje načela zaštite podataka*, kao što je korišćenje najmanjeg mogućeg obima podataka, i u obradu uključuje zaštitne mere radi ispunjenja zahteva iz ove uredbe kako bi se zaštitila prava lica na koja se podaci odnose".

Sam princip obuhvata primenu odgovarajućih tehničkih i organizacionih mera zaštite već *u stadijumu određivanja sredstava obrade* (u fazi planiranja, kreiranja, integracije, uspostavljanja sistema), ali i u fazi *same obrade podataka* do završetka obrade.

U suštini ovog principa je *ne samo implementacija adekvatnih tehničkih i organizacionih mera zaštite* tokom čitavog ciklusa obrade podataka, nego i implementacija *načela zaštite podataka*. Osim toga treba uočiti, iako je navedeno samo kao primer, da je zakonodavac posebno istakao *načelo minimizacije podataka* (čl. 5 st. 1 c) OUZP). Međutim i ovaj primer se može tumačiti kao bitan element za ostvarivanje principa Privacy by Design.

Potencijalne tehničko - organizacione mere zaštite „bi mogle, između ostalog, da se sastoje od svođenja obrade podataka o ličnosti na najmanju moguću meru, pseudonimizacije podataka o ličnosti što je pre moguće, transparentnosti u vezi sa funkcijama i obradom podataka o ličnosti, omogućavanja licu na koje se podaci odnose

[193] Walter Hötzendorfer, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 137, 139, 141.

da prati obradu podataka, omogućavanja rukovaocu podataka da stvara i unapređuje bezbednosne karakteristike“ (U.t.r. 78 OUZP).

Procena proporcionalnosti tehničkih i organizacionih mera zaštite

Potrebno je posebno proceniti koje konkretno tehničke i organizacione mere zaštite treba implementirati. Proporcionalnost mera treba proceniti u odnosu na 4 bitna faktora:

1. Stanje tehnike, odnosno tehnološki razvoj,
2. Troškove sprovođenja i prirodu,
3. Obim, kontekst i svrhe obrade,
4. Rizike u vezi sa obradom (u odnosu na različite stepene verovatnoće i ozbiljnosti potencijalnih ugrožavanja prava i sloboda fizičkih lica).

Identičnu procenu proporcionalnosti mera nalazimo u članu 32 OUZP. Upravo ovakve nejasne formulacije ostavljaju prostora za različita tumačenja u praksi, te je stoga od slučaja do slučaja potrebno proceniti koje mere treba preduzeti.

U praksi bi se trebalo zapitati u čitavom ciklusu sistema (od planiranja do programiranja funkcija), da li su konkretne informacije neophodne za ostvarenje svrhe? Koliko dugo su potrebne informacije? Kome su sve potrebne informacije? Da li postoji mogućnost decentralizovanog čuvanja podataka i odvajanja podataka?

Isto tako čl. 25 i čl. 32 OUZP imaju za cilj *primenu tehničkih i organizacionih mera zaštite*, s tim što je kod čl. 25 primena zaštitnih mera samo jedan od ciljeva pošto je za ostvarivanje principa Privacy by Design neophodno *i ostvarenje načela zaštite podataka* (čl. 5 OUZP). Sam član 32 OUZP služi ostvarivanju *načela bezbednosti podataka* (čl. 5 st. 1 f) OUZP) te stoga i preduzimanje adekvatnih mera zaštite treba posmatrati u kontekstu ispunjenja načela zaštite podataka.[194]

7.2. Privacy by default

Čl. 25 st. 2 OUZP definiše princip Privacy by Default: „Rukovalac primenjuje odgovarajuće *tehničke i organizacione mere kojima se obezbeđuje* da se podrazumevana obrada vrši samo nad podacima o ličnosti koji su neophodni za konkretnu svrhu obrade. Ova obaveza se odnosi na količinu prikupljenih podataka o ličnosti, obim njihove obrade, rok njihovog čuvanja i njihovu dostupnost. Konkretno, tim merama se obezbeđuje da podaci o ličnosti ne budu automatski, bez intervencije lica, dostupni neograničenom broju fizičkih lica“.

I kod ovog principa imamo implementaciju adekvatnih tehničko-organizacionih mera zaštite, koju treba obezbediti od strane rukovaoca. Obezbeđivanje treba ostvariti putem dokumentovanja, što bi se u praksi pre svega odnosilo na dokumentovanje procesa.

[194] *Ibidem*, str. 142, 143, 144.

U zadnjoj rečenici ovog principa se zahteva da same postavke ne budu automatski napravljene, na taj način da podaci o ličnosti budu dostupni širokom broju ljudi. Tipičan primer kršenja ovog principa su profili korisnika Fejsbuka koji su po difoltu otvoreni. Identičan primer je i postavljanje slika na ovu društvenu mrežu, pošto slike ne bi smele po difoltu da budu dostupne široj javnosti, već da korisnici sami odrede sa kim žele da ih podele.

Za razliku od principa Privacy by Design kod principa Privacy by Default nije neophodno da se izvrši procena proporcionalnosti tehničkih i organizacionih mera zaštite. *Ovaj princip treba primeniti nezavisno od troškova, rizika i ostalih faktora.* U praksi je ova odredba problematična iz razloga što se može sa izvesnošću tvrditi da stari sistemi nemaju podrazumevane opcije u svrhu zaštite podataka o ličnosti. Stoga bi praktično ova odredba zahtevala ili zamenu sistema ili teško ostvarivu adaptaciju postojećih rešenja. To bi pre svega u praksi značilo adaptaciju rešenja vezanih za prikupljanje „kolačića" (eng. cookies) putem veb stranica u vidu toga da su kolačići u statističke svrhe, marketinške svrhe, profilisanje, unapred isključeni (izuzev neophodnih kolačića za funkcionalnost veb sajta).

Kao jedno od mogućih *načina dokazivanja ispunjenja principa Privacy by Design i Privacy by Default* (čl. 25 st. 3 OUZP) je *mehanizam sertifikacije iz člana 42 OUZP*. Radi se o mehanizama sertifikacije zaštite podataka, pečata i oznaka za zaštitu podataka (garancije kvaliteta). Treba naglasiti da se radi samo o mogućim načinima dokazivanja, a ne i obavezi za rukovaoce.

Može se uočiti da obaveza usklađenost sa OUZP u pogledu Privacy by Design i Privacy by Default pogađa isključivo rukovaoca. To je naravno sa stanovišta ostvarivanja ovih principa važno naglasiti, ali uočiti i razliku u odnosu na stadijum primene. Naime proizvođači softvera imaju uticaj na oblikovanje proizvoda u smislu principa Privacy by Design i Privacy by Default, što za većinu rukovaoca u kasnijim fazama po kupovini softvera najčešće nije moguće. Stoga su ovim principima pre svega u smislu korišćenja standardnih softvera pogođeni *proizvođači softvera*.

O tome govori i OUZP u U.t.r. 78 „*proizvođače proizvoda, usluga i aplikacija* treba podsticati da uzmu u obzir pravo na zaštitu podataka *prilikom razvijanja i osmišljavanja takvih proizvoda, usluga i aplikacija* i da, uzimajući u obzir najnoviji tehnološki razvoj, obezbede da rukovaoci i obrađivači budu u mogućnosti da ispune svoje obaveze u vezi sa zaštitom podataka".

U svakom slučaju od rukovaoca pre svega se zahteva da svoje procese prilagodi primeni ovih principa i da se od starta uzmu u obzir pre svega relevantna načela zaštite podataka kao i tehničko-organizacione mere zaštite.[195]

[195] *Ibidem,* str. 146, 150.

8. EVIDENCIJA AKTIVNOSTI OBRADE (čl. 30 OUZP)

8.1. Uloga i obaveza vođenja evidencija

Vođenje evidencija aktivnosti obrade podataka ima za cilj da pokaže *usklađenost rukovaoca ili obrađivača sa OUZP* (U.t.r. 82 OUZP). Takođe još jedan od ciljeva je da se omogući *nadzornim organima uvid u evidenciju*.

Iz evidencije se da sa priličnim stepenom verovatnoće zaključiti usklađenost rukovaoca ili obrađivača sa OUZP. Do sada su organizacije bile u obavezi da prijavljuju u centralni registar aktivnosti obrade podataka, a ovaj centralni registar je služio u svrhu pružanja informacija pojedincima. Od stupanja na snagu OUZP ova obaveza se ostvaruje interno u organizaciji, a prava pojedinaca u pogledu informacija su pooštrena i proširena.

Vođenje evidencija aktivnosti obrade podataka po OUZP predstavlja obavezu ne samo za *rukovaoce* već i za *predstavnike rukovaoca* (čl. 4 tč. 17 OUZP) i za *obrađivače kao i* za *predstavnike obrađivača* (čl. 4 tč. 17 OUZP). Kod obrađivača treba pravilno odrediti u kom svojstvu istupa organizacija, pošto i obrađivač može imati svoje klijente i zaposlene, i kada deluje kao rukovalac.

Stoga organizacija koja pre svega ima ulogu obrađivača mora da vodi duplu evidenciju aktivnosti obrade podataka:

- ✓ Kao rukovalac za svoje podatke
- ✓ Kao obrađivač, gde deluje po nalogu svojih klijenata

Treba imati u vidu da obaveza vođenja evidencije *ni na koji način ne pogađa ovlašćeno lice za zaštitu podataka*. I na ovaj način je jasno pokazano stanovište OUZP, da ovlašćeno lice za zaštitu podataka ima pre svega kontrolnu i nadzornu ulogu u organizaciji. Svakako da, interno zavisno od okolnosti, i ovlašćeno lice može da vodi evidenciju aktivnosti obrade, ali bi to npr. kod eksternog ovlašćenog lica za zaštitu podataka bilo teško izvodljivo.

8.2. Izuzeci od obaveze vođenja evidencija

Obaveza vođenja evidencija o procesima obrade se ne primenjuje (čl. 30 st. 5 OUZP) ‘‘na preduzeće ili organizaciju u kojoj je zaposleno manje od 250 lica, osim kada postoji verovatnoća da će obrada koju vrši predstavljati visok stepen rizika za prava i slobode lica na koja se podaci odnose, ako obrada nije povremena ili ako obrada obuhvata posebne kategorije podataka iz člana 9, stav 1. ili su u pitanju podaci o ličnosti koji se odnose na krivičnu i prekršajnu osuđivanost iz člana 10’’. U Ut.r. 13 OUZP kaže se ‘‘Ova uredba sadrži izuzetke za organizacije sa manje od 250

zaposlenih u vezi sa vođenjem evidencije, da bi se uzela u obzir posebna situacija u kojoj se nalaze mikro, mala i srednja preduzeća".

Samo razjašnjavanje izuzetaka od obaveza vođenja evidencije predstavlja bitan preduslov, da bi rukovaoci i obrađivači bili u stanju da procene, da li ih pogađa obaveza vođenja evidencije o procesima obrade podataka.

Da bi došlo do izuzetka od vođenja evidencije generalno *je potrebno da bude manje od 250 zaposlenih*. OUZP ne pravi razliku da li se radi o zaposlenima sa punim radnim vremenom, ili o zaposlenima koji rade pola radnog vremena. Pritom se takođe ne pravi razlika da li su u pitanju službenici ili radnici. Svaki zaposleni se računa nezavisno od statusa (to važi i za pozajmljenu radnu snagu).

Postoje 3 situacije kada su rukovaoci i obrađivači u obavezi da vode evidencije o aktivnostima obrade podataka. Ove situacije su postavljene *alternativno*, tako da je *dovoljno da je jedna od situacija primenljiva, da bi došlo do obaveze vođenja registra*.

Ove situacije su:

- ✓ Kada se radi o obradi koja će *verovatno dovesti do visokog rizika za prava i slobode pojedinaca*.
- ✓ Kada se radi o *obradi koja nije povremena*.
- ✓ Kada se radi o obradi koja uključuje *posebne kategorije podataka* ili *podatke* o ličnosti koji se odnose na *krivične presude i krivična dela*.

Sama situacija da će obrada verovatno dovesti do visokog rizika dovoljan je osnov da postoji obaveza vođenja evidencije za rukovaoca i obrađivača. Takođe pojam rizika po prava i slobode pojedinaca nije jasan, ali treba poći od stanovišta da se odnosi na sve moguće rizike. Ostaje u praksi da se pokaže svrsishodnost ovog dela odredbe, pošto praktično ne postoji obrada podataka koja sa sobom ne nosi neku vrstu rizika. Čak i samo sužavanje na prava i slobode pojedinca u odnosu na rizik ne rešava navedenu problematiku, jer takođe svaka povreda prava zaštite podataka po sebi utiče na slobodu i prava pojedinaca.[196]

Isto tako obaveza vođenja evidencije važi i u situacijama kada se radi o obradi, koja nije privremena kao i u situacijama kada se radi obradi posebnih kategorija podataka. Neke obrade podataka se obavljaju redovno, a neke povremeno. Ukoliko se radi o obradi koja je stalna (npr. obrada podataka u svrhu isplata zarada zaposlenih), tada ovaj uslov nije ispunjen.

Povremene obrade bi bile situacije koje se dešavaju npr. jedanput godišnje ili retko. To su situacije proslava i određenih dešavanja, koja nisu redovna. Periodična dešavanja bi bila diskutabilna i mogla bi dovesti do situacije da ovaj izuzetak ne važi.

Tako da po mišljenju Radne grupe član 29, *iako postoji manje od 250 zaposlenih*, rukovaoci i obrađivači koji obrađuju podatke,

[196] Robert Selk*, Datenschutz-Grundverordnung,* Knyrim, 2016., str. 184, 185.

- ✓ koji će verovatno rezultirati rizikom (*a ne samo visokim rizikom*) po pojedince ili
- ✓ se radi obradi koja nije privremena ili
- ✓ se radi obrade posebnih kategorija podataka (čl. 9 st. 1 OUZP) ili o podacima koji se odnose na krivične presude i krivična dela (čl. 10 OUZP)

dužni su da vode evidenciju o aktivnostima obrade podataka.

Organizacije koje imaju manje od 250 zaposlenih pogađa ova obaveza samo u ova 3 slučaja aktivnosti obrade podataka.

U praksi će postojati mala kompanija, koja ima manje od 250 zaposlenih, a koja redovno obavlja obradu podataka svojih zaposlenih. Takva obrada se ne može smatrati „povremenom". Te stoga postoji obaveza za rukovaoce da ove aktivnosti obrade evidentiraju. Sa druge strane ostale aktivnosti koje su povremene, ne treba da budu evidentirane. Međutim obaveza vođenja evidencija postoji i u slučajevima da postoje povremene aktivnosti obrade, ali se radi o obradi podataka koja verovatno može dovesti do visokog rizika ili ako se obrađuju posebne kategorije podataka (čak i povremeno) ili o podacima koji se odnose na krivične presude i krivična dela (čak i povremeno).

Isto tako čak i u slučaju da organizacija ima manje od 250 zapolenih, ali ako pritom obrađuje npr. podatke o zdravlju, moraće da vodi evidenciju.

Stiče se utisak uzimajući u obzir sve izuzetke, da praktično *ne postoji situacija u kojoj bi neka organizacija u celosti bila oslobođenja vođenja evidencije aktivnosti obrade podataka*. Ti izuzeci bi bili mogući za posebne obrade podataka, koje pre svega ne predstavljaju nikakav rizik po sebi.

Evidencija aktivnosti obrade predstavlja veoma korisno sredstvo za analizu procene uticaja bilo koje obrade, nevezano za to da li se radi o postojećoj ili planiranoj obradi. Na taj način evidencija olakšava procenu rizika za rukovaoce ili obrađivače, kao i identifikaciju odgovarajućih tehničkih i organizacionih mera. A sve to naravno utiče na ispunjavanje načela društvene odgovornosti (čl. 5 st. 2 OUZP).[197]

8.3. Forma evidencija aktivnosti obrade podataka

Ni ovo pitanje nije detaljno regulisano u OUZP, ali se da zaključiti da je neophodno fizički napraviti dokument o tome. Shodno OUZP taj dokument (čl. 30 st. 3 OUZP) bi trebalo da bude u *pisanoj, elektronskoj formi* (word, excel, power point, share point, ali i ostali softveri).

---

[197] *Dokument o stavu Radne grupe član 29 u vezi sa izuzecima od obaveze vođenja evidencija o aktivnostima obrade u skladu sa članom 30 stav 5 OUZP*, Working party 29 Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR, str. 1, 2.

S obzirom da je regulisana obaveza za rukovaoca ili obrađivača i predstavnika rukovaoca ili obrađivača, da „*na zahtev omogućavaju nadzornom organu uvid u evidenciju*“ (čl. 30 st. 4 OUZP), jasno je da evidencija mora u fizičkom smislu biti prisutna kako bi dokument bio ili poslat ili pokazan nadzornom organu.

8.4. Sadržaj evidencija aktivnosti obrade podataka uopšteno

Najpre treba ustanoviti šta se upisuje u evidenciju aktivnosti obrade podataka. Uočljivo je da OUZP govori o „*aktivnosti obrade*“ (čl. 30 st. 1 OUZP) a ne o „obradi“ (kako je definisano u čl. 4 tč. 2 OUZP). Ipak u definiciji obrade OUZP govori da je to „svaki postupak“, te stoga bi se postupak i aktivnost jezički mogli smatrati identičnim značenjem. To podrazumeva *da treba obuhvatiti svaki postupak odnosno svaku aktivnost obrade i opisati u evidenciji*.

Da li se ta aktivnost odnosi npr. na samo aktivnosti obrade kadrovskog odeljenja ili te aktivnosti obuhvataju svaki mogući postupak u kadrovskom odeljenju od prijave za posao, izrade svedočanstava, isplata premija, odobravanja odmora...., OUZP ne daje odgovor na to pitanje. Ukoliko se uzme u obzir baš svaka aktivnost obrade, to naravno može biti preopširno, stoga se preporučuje da evidencija ne bude ni previše detaljna, a ni previše skromnog sadržaja. Osim toga u praksi se kao dobra pokazala metodika da se aktivnosti obrade prikupljaju i opisuju po odeljenjima (npr. marketing, kadrovsko, nabavka itd.).[198]

Kao smernice u izradi evidencija aktivnosti obrade mogu poslužiti sledeći kriterijumi:

- ✓ *Pravna sudbina podataka* – obrade se tako popišu i obuhvate u onim situacijama u kojima su one potrebne za npr. zaključenje ugovora, njegovo sprovođenje i okončanje. *Primeri:* Podaci klijenata, podaci zaposlenih, pošto sa ovim kategorijama skoro redovno postoji ugovorni odnos.
- ✓ *Životni ciklus podataka* – od samog prikupljanja do brisanja. Ovaj pristup je primenljiv u tehničkom okruženju npr. kod log fajlova, prijava na sistem. Tako bi po ovom metodu bilo moguće podeliti podatke klijenata po fazama npr. faza akviriranja, faza aktivnog ugovora i odnosa sa klijentom i na kraju faza okončanja saradnje sa klijentima.

Faza akviriranja bi bila obrada podataka koja predhodi samom ugovoru sa klijentom, slanje ponude i sve generalno predugovorne radnje.

Faza aktivnog ugovora i odnosa sa klijentom bi bila obrada isplata usluga, naplata potraživanja, pruženje usluga i servisa itd.

Faza okončanja saradnje sa klijentima bi bio postupak brisanja podataka ili vraćanja dokumentacije, uređaja itd.

---

[198] Robert Selk*, Datenschutz-Grundverordnung,* Knyrim, 2016., str. 187, 188.

Ove kategorije je moguće po potrebi dalje razgraditi na podkategorije, ali treba imati u vidu da se ne ide previše u detalje i u podatke koji su već obuhvaćeni. Osim toga sa druge strane potrebno je obuhvatiti sve aktivnosti obrade.

8.5. Sadržaj evidencija aktivnosti obrade podataka rukovaoca (čl. 30 st. 1 OUZP)

U pogledu sadržaja evidencija aktivnosti obrade podataka koju vodi rukovalac evidencija mora da obuhvati:

- ✓ *Ime i kontakt podatke rukovaoca i ukoliko je primenljivo, zajedničkog rukovaoca, predstavnika rukovaoca i ovlašćenog lica za zaštitu podataka* (čl. 30 st. 1 a) OUZP).

Kao što se može zaključiti iz ovoga neophodno je navođenje imena i kontakt podataka rukovaoca, dok su svi ostali podaci po potrebi neophodni, odnosno ako se to dotične organizacije tiče. To bi značilo ako postoji ovlašćeno lice za zašitu podataka u organizaciji, treba navesti njegove podatke. Ukoliko u određenim situacijama obrade postoji više rukovaoca i to treba zabeležiti u evidenciji. Takođe ako se radi o predstavniku rukovaoca u EU (čl. 27 OUZP) i njegove podatke treba navesti.

- ✓ *Opis svrhe obrade* (čl. 30 st. 1 b) OUZP).
  To bi značilo da se po aktivnosti, odnosno postupku obrade opisuje konkretna svrha, koju treba što detaljnije i preciznije opisati. Na osnovu te svrhe se dalje određuje zakonska dopuštenost obrade podataka.
- ✓ *Opis kategorija lica na koja se podaci odnose i kategorija podataka o ličnosti* (čl. 30 st. 1 c) OUZP).
  Ovde treba imati u vidu da se radi o konkretnim *kategorijama podataka* kao što su npr. „kontakt podaci zaposlenih“, *a ne* „ime, prezime, adresa stanovanja, tel. broj itd.“. Ne radi se o pojedinim poljima podataka, već o kategoriji. Navođenje pojedinih vrsta podataka ili polja podataka bi bilo svakako poželjno za razumevanje aktivnosti obrade, ali nije neophodno shodno OUZP.
  Identično važi i za situacije o rukovaočevim podacima klijenata, gde bi npr. kategoriju predstavljali „kontakt podaci klijenata“.
- ✓ *Kategorije korisnika* kojima su podaci o ličnosti otkriveni ili će im biti otkriveni, uključujući i *korisnike u trećim zemljama ili međunarodne organizacije* (čl. 30 st. 1 d) OUZP).
  „Korisnik” je fizičko ili pravno lice, organ vlasti, agencija ili drugo telo kojem se otkrivaju podaci o ličnosti, nezavisno od toga da li je u pitanju treće lice ili ne (čl. 4 tč. 9 OUZP). Korisnik može biti neko odeljenje u okviru firme (marketing, HR, IT itd.), a može biti i pravno lice (firma dobavljač,

banka, osiguravajuće društvo, poslovni partner), državna institucija (sud, organ uprave itd.).
U praksi se ove kategorije lako razaznaju i mogu se opisati uz pomoć koncepta ovlašćenja za pristup određenom sistemu.
Veoma je važno da se po kategoriji primaoca takođe navede, da li se podaci *prenose u treće zemlje ili međunarodne organizacije.* U ovom slučaju se preporučuje da se navedu u evidenciji koje zemlje važe kao „sigurne", a koje su onda ostale „treće zemlje".

- ✓ *Informacije o prenosu podataka o ličnosti u treću zemlju ili međunarodnu organizaciju, sa identifikacijom te treće zemlje ili međunarodne organizacije i, u slučaju prenosa iz člana 49, stav 1, drugi podstav, sa dokumentacijom o odgovarajućim zaštitnim merama* (čl. 30 st. 1 e) OUZP).
  U ovom slučaju se radi za razliku od predhodnog zahteva o detaljnijim informacijama, ukoliko se podaci prenose u teće zemlje ili međunarodne organizacije, tada je potrebno pružiti i *informacije o zakonskom osnovu* iz čl. 49 st. 1 OUZP *i dokumentovati i opisati mere zaštite*.
- ✓ *Ako je moguće rokove za brisanje različitih kategorija podataka* (čl. 30 st. 1 f) OUZP).
  Rok za brisanje podataka treba predvideti po kategoriji podataka. Pritom se radi o konkretnim rokovima za brisanje podataka. U praksi se preporučuje izrada *koncepta brisanja podataka*, u kojem bi detaljno bilo opisano kad koji podaci trebaju da budu obrisani.
- ✓ *Ako je moguće opšti opis tehničkih i organizacionih bezbednosnih mera iz čl. 32 st. 1* (čl. 30 st. 1 f) OUZP).
  Najčešće se tehničko - organizacione mere ne odnose na same kategorije podataka već na jednu obradu ukupno. U praksi se pokazalo, da su stoga neki rukovaoci upućivali na dokumenta gde su bliže opisane mere zaštite. To se takođe preporučuje, pošto se mere zaštite konstantno unapređuju u prilagođavaju standardu i stanju tehnike. U tom slučaju se izbegava konstantna adaptacija evidencija aktivnosti obrade podataka.[199]

8.6. Sadržaj evidencija aktivnosti obrade podataka obrađivača (čl. 30 st. 2 OUZP)

Kao što smo već konstatovali i obrađivač je u obavezi da vodi evidenciju aktivnosti obrade podataka za svoje klijente. Za razliku od rukovaoca, obrađivač mora da vodi samo kategorije podataka koje obrađuje po nalogu rukovaoca, a ne i pojedine aktivnosti obrade.

Po kategorijama obrađivači su dužni da vode:

[199] *Ibidem*, str. 191, 192.

- ✓ *Ime i kontakt podatke obrađivača ili zajedničkog obrađivača, svakog rukovaoca u čije ime obrađivač deluje, a u odgovarajućim slučajevima i predstavnika rukovaoca ili obrađivača i ovlašćenog lica za zaštitu podataka* (čl. 30 st. 2 a) OUZP).

U odnosu na rukovaoca i st. 1 ovde dolazi samo do unosa dodatne kategorije obrađivača, za koju je angažovan od strane rukovaoca.

- ✓ *Kategorije obrade koje se obavljaju u ime svakog rukovaoca* (čl. 30 st. 2 b) OUZP).

Potrebno je da se po obrađivaču vodi evidencija u kojoj će biti opisana svaka kategorija obrade.

- ✓ *Informacije o prenosu podataka o ličnosti u treću zemlju ili međunarodnu organizaciju, sa identifikacijom te treće zemlje ili međunarodne organizacije i, u slučaju prenosa iz člana 49, stav 1, drugi podstav, s dokumentacijom o odgovarajućim zaštitnim merama* (čl. 30 st. 2 c) OUZP).

Ovo je identični zahtev kao i za rukovaoca iz st. 1.

- ✓ *Ako je moguće opšti opis tehničkih i organizacionih bezbednosnih mera iz čl. 32 st. 1* (čl. 30 st. 2 d) OUZP).

I ovo je identični zahtev kao i za rukovaoca iz st. 1, ali kao pomoć može poslužiti ugovor sa rukovaocem, gde su mere zaštite opisane.[200]

[200] *Ibidem*, str. 196, 197.

9. BEZBEDNOST OBRADE PODATAKA (čl. 32 OUZP)

Bezbednost podataka je jedno od načela zaštite podataka o ličnosti (čl. 5 st. 1 f) OUZP), koje sadrži u sebi dva od tri osnovna principa bezbednosti informacija „*integritet*" (celovitost informacija) i „*poverljivost*". Uočljivo je da princip „dostupnosti" informacija nedostaje.

Razlog izostavljanju ovog bitnog principa bi mogao biti pre svega u tome, što bi on stajao direktno ili indirektno u suprotnosti sa načelom „ograničenja čuvanja" (čl. 5 st. 1 e) OUZP) zbog svog glavnog zahteva da informacije uvek budu dostupne. Princip dostupnosti kao i ostale principe integritet i povreljivost nalazmo u čl. 32 OUZP, koji zapravo *predstavlja sprovođenje načela bezbednosti podataka*. Da bi se osigurala i obezbedila bezbednost podataka potrebno je poceniti rizik i primeniti odgovarajuće tehničko - organizacione mere (čl. 32 st. 1 OUZP). Ove obaveze *pogađaju i rukovaoca i obrađivača*.

Kriterijumi za procenu rizika su stepen verovatnoće i ozbiljnosti za prava i slobode fizičkih lica koji proizilaze iz obrade podataka.

Kriterijumi za primenu tehničko - organizacionih mera su tehnološki razvoj, troškovi sprovođenja i priroda, obim, kontekst i svrhe obrade.

Kada se uzme u obzir intencija zakonodavca, može se zaključiti da je preduslov za obezbeđivanje bezbednosti podataka o ličnosti procena rizika. Tako OUZP *pored navedenih kriterijuma za procenu rizika navodi da treba posebno uzeti u obzir* rizike od slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja podataka o ličnosti ili neovlašćenog pristupa podacima o ličnosti koji su preneti, sačuvani ili na drugi način obrađivani (čl. 32 st. 2 OUZP). Mere zaštite treba da *služe sprečavanju kršenja bezbednosti podataka o ličnosti „eng. Data Breach"* (čl. 4 tč. 12 OUZP).

Do sada u pravu zaštite podataka nije bilo navođenja konkretnih mera za zaštitu bezbednosti podataka, već je bilo navođenja pravnih standarda kao što je „stanje tehnike". Donošenjem OUZP mere su konkretizovane (ali opet dovoljno fleksibilne).

Mere zaštite koje predviđene OUZP su:

- ✓ pseudonimizacija i enkripcija;
- ✓ obezbeđivanje trajne poverljivosti, celovitosti, dostupnosti i otpornosti sistema i usluga obrade;
- ✓ sposobnost blagovremenog ponovnog uspostavljanja dostupnosti podataka o ličnosti i pristupa njima u slučaju fizičkog ili tehničkog incidenta;
- ✓ postupak redovnog testiranja, ocenjivanja i procene delotvornosti tehničkih i organizacionih mera za postizanje bezbednosti obrade.

O bezbednosnoj meri *pseudonimizacije* je već bilo reči kod definicija (poglavlje 2.5).

Enkripcija je metoda zaključavanja odnosno šifriranja informacija. Ona predstavlja jedan kriptografski proces, kojim se vrši izmena podataka tako da se

poruka, odnosno informacije, učine nečitljivim za osobe koje ne poseduju ključ (najčešće šifru ili kod).

Danas se svakodnevno izrađuju, šalju i snimaju ogromne količine podataka. Da bi se ovi podaci zaštitili od neželjenih pristupa potrebno ih je enkriptovati (zaključavati, šifrirati). Enkripcija se koristi kako za snimanje/čuvanje podataka tako i za *slanje podataka* preko svih kanala komunikacije.

U organizacijama je potrebno predhodno klasifikovati podatke, kako bi se definisale klase podataka po svom stepenu zaštite i po tome odredilo ko ima koje pravo pristupa tim podacima. U smislu bezbednosti podataka enkripcija služi u cilju *ostvarenja principa poverljivosti i integriteta* (celovitosti).

Integritet podrazumeva da se informacije mogu promeniti od strane predviđenih osoba i u okviru predviđenih procesa.

Poverljivost podrazumeva da se informacije mogu otkrivati samo predviđenim osobama i u okviru predviđenih procesa.

Dostupnost podrazumeva da informacije moraju da budu dostupne predviđenim osobama i u okviru predviđenih procedura.

Otpornost sistema se pre svega odnosi na tehničke zahteve sistema, koji treba da budu otporni. Jedan tehnički sistem je otporan, onda *kada može većinu očekivanih smetnjih da prevaziđe bez suštinskog ometanja njegove funkcionalne sposobnosti*.[201] Na taj način se IT sistemi ojačavaju da bi se obezbedili od tipičnih pretnji i napada. Tako za ovaj zahtev važi pravilo da treba postoji jedan glavni sistem i još jedan rezervni. Tipični primer je sprovođenja ove mere zaštite je redundantnost (dvostrukost) servera, ali takođe i upotreba anti-virus programa pa i backup sistema.[202]

Sposobnost blagovremenog ponovnog uspostavljanja dostupnosti podataka o ličnosti i pristupa njima u slučaju fizičkog ili tehničkog incidenta odnosi na zahteve u hitnim situacijama. U tu svrhu se preporučuje izrada *priručnika i plana za postupanje u hitnim situacijama*, koji treba da bude deo Business Continuity Management-a. U fokusu ne bi trebalo da bude samo IT, već čitava organizacija, koja treba da omogući brzo i blagovremeno uspostavljanje dostupnosti podataka u slučaju ispada sistema ili povreda bezbednosti uopšte.

Postupak redovnog testiranja, ocenjivanja i procene delotvornosti tehničkih i organizacionih mera za postizanje bezbednosti obrade može se u organizacijama ostvariti uz pomoć *internih ili eksternih audit-a ili kontrola*. U tu svrhu mogu poslužiti i unapred definisane interne kontrolne mere, ali i eksterna kontrola npr. od strane ovlašćenog lica za zaštitu podataka.

Može se primetiti da među pobrojanim merama *nedostaje obuka i trening zaposlenih u organizaciji*. Iako ova obaveza nije izričito predviđena, svakako da

---

[201] Thorsten Kamp, Was ist Belastbarkeit im Sinne von Art. 32 DSGVO?, https://www.datenschutz-notizen.de/was-ist-belastbarkeit-im-sinne-von-art-32-dsgvo-3319778/, 01.11.2018.

[202] Redundantni serveri su spojeni u jednom savezu servera tzv. klustera. Pritom svaki redundantni server ima pristup istoj bazi podataka (podacima i programima) u ovom savezu računara. Klusteri se koriste kako bi povećali dostupnost, karakteristike računara. Ovi duplikati servera utiču na to da u slučaju ispada jednog servera drugi bude u stanju da preuzme funkciju i nastavi normalan rad.

je ona ne samo poželjna nego i *neophodna u smislu dokazivanja preduzetih mera zaštite u organizaciji*, pogotovu imajući u vidu ljudski faktor kao faktor rizika. Takođe iz obaveza ovlašćenog lica za zaštitu podataka, da se zaključiti da je intencija zakonodavca ipak išla u smeru da se rukovodstvo i zaposleni redovno obučavaju "podizanje svesti i osposobljavanje osoblja koje učestvuje u radnjama obrade" (čl. 39 st. 1 b) OUZP).

Rukovalac i obrađivač preduzimaju mere kako bi obezbedili da svako fizičko lice koje deluje na osnovu ovlašćenja rukovaoca ili obrađivača i koje ima *pristup podacima o ličnosti ne obrađuje te podatke bez naloga rukovaoca* (čl. 32 st. 4 OUZP). Ovaj zahtev se odnosi na koncept ovlašćenja i prava pristupa koje rukovalac i obrađivač treba da sprovedu, kako bi obezbedili da samo lica u skladu sa svojim dužnostima obrađuju podatke (princip need to know).

Dokaz preduzetih tehničko-organizacionih mera (čl. 32 st. 3 OUZP) moguće je pribaviti uz pomoć *odobrenih kodeksa ponašanja* (čl. 40 OUZP) ili *odobrenog mehanizma sertifikacije* (čl. 42 OUZP). U svrhu sertifikacije može poslužiti i svakako je za preporuku *uvođenje menadžmenta bebednosti informacija* (information security management system) i *sertifikacija po međunarodnom standardu ISO 27001*. Takođe u ovu svrhu potrebno je koristiti i smernice, preporuke i primere dobre prakse iz ISO 27002.[203]

9.1. Enkripcija prenosa odnosno slanja podataka

Kako bi se podaci na bezbedan način prenosili potrebno je enkripovati kanale komunikacije.

Primeri upotrebe:

- ✓ E-mail serveri (npr. S/MIME, PGP, Gateway),
- ✓ IP (npr. VoIP) i ISDN bazirano telefoniranje (npr. Secure Real-Time Transport Protocol, ZRTP protokol),
- ✓ Messaging usluge (npr. viber, whats up, chat komunikacija; IRC, XMPP protokoli),
- ✓ platforme za saradnju u okviru projekata sa trećim licima (npr. Citrix, WebEx),
- ✓ veb stranice (npr. HTTPS protokol, TLS/SSL protokoli),
- ✓ LAN (npr. MAC-filter, MACsec, WPA2) i VPN (npr. IPsec) veze sa internim serverima.

[203] Hans –Jürgen Pollirer, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 199, 200, 201.

9.2. Enkripcija snimanja odnosno čuvanja podataka

Snimljeni podaci odnosno podaci koji se čuvaju se mogu enkripovati.

Primeri upotrebe:

- ✓ posebni fajlovi (npr. word dokument, acrobat reader),
- ✓ datoteke (moguće je zaključati celu particiju hard diska, kao i posebne foldere),
- ✓ mobilni uređaji (npr. Mobile Device Management),
- ✓ pojedini komponente računara (npr. hard disk),
- ✓ prenosni medijumi (npr. USB, eksterni hard diskovi),
- ✓ moguće je enkripovati podatke u zaključanim tzv. „kontejnerima“,
- ✓ ceo operativni sistem se može enkripovati (npr. Encrypting File System).[204]

[204] Institut für Internetsicherheit und Goldmedia Strategy Consulting, Kompass IT-Verschlüsselung, 20.02. 2018., str. 5, 6, 32.

10. PROCENA RIZIKA (čl. 24 OUZP)

Sam pristup baziran na riziku (čl. 24 OUZP) znači da su rukovaoci generalno u obavezi da: uzmu u obzir vrstu, obim, okolnosti i svrhe obrade, kao i rizike različitih nivoa verovatnoće i težine po prava i slobode pojedinaca kao i da preduzmu odgovarajuće tehničke i organizacione mere kako bi osigurali i dokazali da se obrada sprovodi u skladu sa OUZP. Ove mere treba prema potrebi preispitivati i ažurirati.

Pristup baziran na riziku u oblasti zaštite podataka ne predstavlja novinu, pošto već je postojao u Direktivi o zaštiti podataka u vidu tzv. *predhodne kontrole* (čl. 20 Direktive 95/46/EZ) ili provere podataka pre preduzimanja aktivnosti obrade podataka. Osim toga sama kategorizacija podataka i razlikovanje između „podataka o ličnosti" i „osetljivih podataka" (čl. 9 OUZP) je bazirana na riziku. Procenljivost rizika treba da posluži usklađivanju sa zahtevima OUZP. U praksi to podrazumeva da rukovaoci koji obrađuju podatke niskog rizika neće imati toliko obaveza u primeni OUZP za razliku od onih rukovaoca čija obrada podataka predstavlja visok rizik.

Rizik za prava i obaveze fizičkih lica, različite verovatnoće i ozbiljnosti, može da nastane iz obrade podataka o ličnosti koja bi mogla da prouzrokuje *fizičku, materijalnu ili nematerijalnu štetu*, a posebno: ako ta obrada može da dovede do (U.t.r. 75 OUZP):

- ✓ diskriminacije,
- ✓ krađe identiteta ili prevare,
- ✓ finansijskog gubitka,
- ✓ štete za ugled,
- ✓ gubitka poverljivosti podataka o ličnosti zaštićenih poslovnom tajnom,
- ✓ neovlašćenog obrnutog postupka pseudonimizacije,
- ✓ bilo koje druge značajne ekonomske ili društvene štete;
- ✓ ako lica na koja se podaci odnose mogu da budu uskraćena za svoja prava i slobode ili sprečena u vršenju kontrole nad svojim podacima o ličnosti;
- ✓ ako se obrađuju podaci o ličnosti koji otkrivaju rasno ili etničko poreklo, politička mišljenja, verska ili filozofska uverenja, članstvo u sindikatu i ako je u pitanju obrada genetičkih podataka, podataka o zdravstvenom stanju ili podataka o seksualnom životu ili krivičnim osudama i krivičnim delima;
- ✓ ako se procenjuju lični aspekti, a posebno analiza ili predviđanje aspekata u vezi sa učinkom na poslu, ekonomskim stanjem, zdravljem, ličnim sklonostima ili interesima, pouzdanošću ili ponašanjem, lokacijom ili kretanjem, kako bi se napravili ili koristili lični profili;
- ✓ ako se obrađuju podaci o ličnosti ugroženih fizičkih lica, a posebno dece;
- ✓ ako obrada obuhvata veliku količinu podataka o ličnosti i utiče na veliki broj lica na koje se podaci odnose.

Pored uvođenja načela društvene odgovornosti (čl. 5 st. 2 OUZP), koje je takođe bazirano na riziku, uvedena je po prvi put obaveza sprovođenja procene uticaja

u vezi sa zaštitom podataka (čl. 35 OUZP). Ukoliko dođe do zloupotrebe podataka, rukovalac takođe treba da proceni rizik po prava pojedinaca (čl. 33 i 34 OUZP). U slučajevima da postoji *verovatnoća da postoji visok rizik* za prava i slobode pojedinaca neophodno je informisati pojedince o povredi bezbednosti podataka (čl. 34 OUZP) i neophodno je sprovesti procenu uticaja u vezi sa zaštitom podataka (čl. 35 OUZP). Rukovalac je u obavezi da o povredi bezbednosti podataka informiše nadzorni organ, ako povreda može dovesti do *rizika* po prava i slobode pojedinaca (čl. 33 OUZP).[205]

Obrade sa visokim rizikom mogu biti one obrade koje koriste nove tehnologije ili koje predstavljaju nove vrste radnji obrade i kod kojih rukovalac podataka još nije izvršio procenu uticaja na zaštitu podataka ili koje postanu neophodne s obzirom na vreme koje je prošlo od prvobitne obrade (U.t.r. 89 OUZP).

Takođe same tehničko - organizacione mere za zaštitu podataka (čl. 32 OUZP) treba preduzeti i izabrati u odnosu na procenu rizika za konkretnu obradu. Sama implementacija rešenja zahtevanih po odnovu privacy by design (čl. 25 OUZP) mora da obuhvati predhodnu procenu rizika po pojedince, a poželjno bi bilo da ima integrisanu procenu rizika u vidu tehničkog rešenja.

U pogledu procene rizika OUZP kaže da verovatnoću i ozbiljnost rizika za prava i slobode lica na koje se podaci odnose treba određivati u odnosu na prirodu, obim, kontekst i svrhe obrade. Rizik treba ocenjivati na osnovu objektivne procene kojom se utvrđuje da li postupci obrade podataka uključuju rizik ili visok rizik (U.t.r. 76 OUZP).

Shodno stavu Radne grupe čl. 29 pristup baziran na riziku treba da obuhvati sledeće situacije:

- ✓ Zaštitu osnovnog ljudskog prava na zaštitu podataka, ragulisanog čl. 8 Evropske povelje o osnovnim ljudskim pravima, tako da svaka operacija obrade bude procenjena.
- ✓ Prava pojedinaca (pravo na informaciju, brisanje itd.) treba da se poštuju bez obzira na nivo rizika.
- ✓ U praksi mogu postojati različiti nivoi rizika u kontekstu društvene odgovornosti, ali rukovaoci moraju ostati odgovorni za dokazivanje usklađenosti sa OUZP bez obzira na konkretne rizike po obradu podataka.
- ✓ Sama procena rizika ne sme imati uticaja na osnovna načela obrade podataka, ali sama primena načela treba biti bazirana na rizicima u zavisnosti od prirode i obima.
- ✓ Obaveze rukovaoca (u pogledu procene uticaja u vezi sa zaštitom podataka, obaveštenja o zloupotrebi podataka, primene tehničkih i organizacionih mera, sertifikacije) zavisno od slučaja i konteksta ne bi trebalo da budu primenjene na rukovaoce, koji obrađuju podatke niskog rizika i malog obima.

[205] Andrea Lehky, DSGVO: Das Risiko der Risikoabschätzung, https:// diepresse.com/ home/ karriere/ karrierenews/ 5381250/ DSGVO _ Das - Risiko - der -Risikoabschaetzung?direct=5373040&_vl_backlink=/home/karriere/karrierenews/5373040/index.do&selChannel=, 31.11.2018.

- ✓ Obim dokumentacije može se razlikovati od visine rizika. Preporučuje se zbog mogućnosti kontrole od strane nadležnog organa za zaštitu podataka, kao i iz razloga transparentnosti u vidu implementacije prava pojedinaca, čiji se podaci obrađuju.
- ✓ Rizici treba da obuhvate procenu uticaja u vezi sa zaštitom podataka uzimajući u obzir kriterijume kao što su priroda podataka (osetljivi podaci ili ne), broj pojedinaca (veliki, srednji, mali), svrha obrade. Osim toga potrebno je proceniti težinu i verovatnoću uticaja na prava i slobode pojedinaca.
- ✓ Procena rizika treba da obuhvati konflikt između osnovnih prava (npr. između prava zaštite podataka i prava na slobodu mišljenja, između prava zaštite podataka i autorskih prava itd.).
- ✓ Kada postoji visok rizik potrebno je preduzeti odgovarajuće dodatne mere zaštite (ovo proizlazi iz obaveza rukovaoca pri proceni uticaja u vezi sa zaštitom podataka, poboljšanje bezbednosnih mera, kada se radi o obaveštavanju o zloupotrebi podataka) i konsultovati ovlašćeno lice za zaštitu podataka ako postoji visok rizik po sprovedenom postupku procene uticaja u vezi sa zaštitom podataka.
- ✓ Sama upotreba tehničkih mera pseudonimizacije ili kriptografije može poslužiti u svrhu smanjenja rizika po pojedince. Iako su ove mere od izuzetnog značaja za zaštitu podataka i mogu se uzeti u obzir prilikom ocenjivanja usaglašenosti sa OUZP, sama njihova upotreba nije dovoljna da oslobodi rukovaoca od odgovornosti.
- ✓ Pristup zasnovan na riziku je baziran na štetama i stvarnim kao i potencijalnim efektima po pojedince za konkretnu obradu uzimajući u obzir i opšti društveni uticaj (npr. u vidu gubitka društvenog poverenja).[206]
- ✓ Procenu rizika treba obuhvatiti i u slučaju procene „opravdanih interesa“, pre svega iz razloga oslobađanja rukovaoca od odgovornosti i transparentnosti po pojedince. Važno je napomenuti da je Radna grupa čl. 29 u ovom dokumentu smatrala da procena rizika nije relevantna za uzimanje u obzir čiji su interesi pretežniji. Sa druge strane to stoji u suprotnosti za mišljenjem 06/2014 o pretežnijim interesima rukovalaca shodno čl. 7 Direktive 95/46/EZ.
- ✓ Ovlašćeno lice za zaštitu podataka sprovodi generalno svoje dužnosti u pogledu procene rizika. Konkretno pristup zasnovan na riziku ovlašćeno lice za zaštitu podataka primenjuje kod procene uticaja u vezi sa zaštitom podataka.[207]

---

[206] Radi se zapravo o gubitku reputacije rukovaoca.

[207] Objašnjenje 14/EN WP 218 Radne grupe čl. 29 o ulozi koncepta rizika u odnosu na reforme o zaštiti podataka, 30. maj 2014., Erklärung 14/EN WP 218 der Datenschutzgruppe über die Rolle eines risikobasierten Ansatzes zu den am 30. Mai 2014 angenommenen Rechtsformen des Datenschutzes, angenommen am 30.05.2014., str. 2, 3, 4.

11. PROCENA UTICAJA U VEZI SA ZAŠTITOM PODATAKA (čl. 35 OUZP)

11.1. Upotreba

Shodno OUZP rukovaoci moraju da preduzmu adekvatne mere, kako bi osigurali i dokazali, da se obrada podataka sprovodi u skladu sa OUZP, pri čemu je neophodno „da se uzmu u obzir *stepen verovatnoće kao i mogućnost nastupanja rizika po prava i slobode pojedinaca*“ (čl. 24 st. 1 OUZP). Ova obaveza podrazumeva adekvatan *menadžment podataka*, da bi došlo do procene rizika. Sama procena rizika se odnosi na događaj i posledice koje proizlaze iz tog događaja po osnovu procene težine i stepena verovatnoće. Procena rizika obuhvata odgovarajuće mere kao i upravljanje rizicima.

Procena uticaja u vezi sa zaštitom podataka predstavlja postupak procene rizika po prava i slobode pojedinaca kao i ispitivanje zaštitnih mera, koje se odnose na obradu podataka o ličnosti. Pored toga ovaj postupak obuhvata i procenu neophodnosti i proporcionalnosti obrade podataka o ličnosti. Postupak procene uticaja u vezi sa zaštitom podataka omogućava rukovaocima da *dokažu usaglašenost sa OUZP i da su adekvatne mere zaštite preduzete*.

Shodno pristupu baziranom na riziku, procenu uticaja u vezi sa zaštitom podataka nije neophodno sprovoditi za sve postupke obrade. Postupak procene uticaja u vezi sa zaštitom podataka *neophodno* je sprovesti, ukoliko obrada podataka može prouzrokovati *visok rizik* za prava i slobode pojedinaca (čl. 32 st. 1 OUZP). To naravno ne isključuje upotrebu mera zaštita i procenu rizika za ostale postupke obrade podataka, koje ne prouzrokuju visok rizik. Da bi rukovalac bio u stanju da proceni visok rizik, mora generalno da proceni rizik za postupke obrade podataka.

Procena uticaja u vezi sa zaštitom podataka može se odnositi na *više sličnih postupaka obrade* koji predstavljaju slične visoke rizike (čl. 35 st. 1 OUZP). Generalno cilj procene uticaja u vezi sa zaštitom podataka je da se ispitaju *nove situacije*, koje bi mogle da predstavljaju visok rizik po prava i slobode pojedinaca. Stoga već ispitane procene rizika ne bi bilo obavezno sprovoditi (npr. u slučaju da se ista vrsta podataka prikuplja u iste svrhe uz upotrebu slične tehnologije).

PRIMER
Više rukovaoca žele da pokrenu sistem video nadzora, koji je baziran na sličnoj tehnologiji. U ovom slučaju nije potrebno obaviti dve procene po posledice pojedinaca, već je dovoljno obaviti jednu procenu. Pri obrazloženju primene zaštitnih mera treba navesti razloge, zbog čega je sprovedena samo jedna procena uticaja u vezi sa zaštitom podataka.

Procena rizika treba da obuhvati ne samo određene *projekte*, već i situacije u kojima *postoji više rukovaoca*. U slučaju više rukovaoca potrebno je jasno definisati odgovornost svakog rukovaoca ponaosob, kao i to koji je rukovalac nadležan za koje mere zaštite.

Upotreba procene uticaja u vezi sa zaštitom podataka može biti od koristi, kada se želi *proceniti uticaj tehnologije na zaštitu podataka*. To se naročito odnosi na situacije u kojima hardver ili softver treba primeniti na različite situacije obrade podataka. Takođe procenu uticaja u vezi sa zaštitom podataka treba primentiti uvek pri upotrebi *novih tehnologija*.[208]

11.2. Obaveza sprovođenja procene uticaja u vezi sa zaštitom podataka

Procenu uticaja u vezi sa zaštitom podataka neophodno je sprovesti ukoliko obrada podataka može prouzrokovati *visok rizik* za prava i slobode pojedinaca, a posebno u sledećim situacijama (čl. 35 st. 3 OUZP):

- ✓ *Sistematke i obimne procene ličnih aspekata* u vezi sa pojedincima, koja se bazira na automatskoj obradi podataka, uključujući izradu profila (profilisanje), i na osnovu koje se donose odluke, koje proizvode pravna dejstva za pojedince ili na sličan način značajno utiču na pojedince;
- ✓ *Obrada u velikoj meri posebnih kategorija podataka* o ličnosti iz člana 9 stav 1 ili podataka u vezi sa krivičnim presudama i krivičnim delima iz člana 10; ili
- ✓ *Sistematski i u velikoj meri nadzor* javno dostupnih prostora.

Postoje situacije koje nisu navedene kao primer u OUZP, a koje takođe proizvode visoke rizike. Za ovakve obrade treba takođe sprovesti procenu posledica po pojedince. To su pre svega obrade vezane za podatke dece.

PREPORUKA
U slučaju da nije jasno, da li je potrebno ili nije potrebno sprovesti procenu uticaja u vezi sa zaštitom podataka, preporučuje se da se uradi procena. To se preporučuje pogotovu iz razloga dokazivanja usaglašenosti sa OUZP, a sama procena predstavlja podesno sredstvo za to.

Procena uticaja u vezi sa zaštitom podataka mora da se sprovede i za obrade podataka koje se već sprovode, samo ukoliko je verovatno da postoji *visok rizik* po prava i slobode pojedinaca. Takođe procena treba da se sprovede, ukoliko su se *rizici promenili* u pogledu vrste, obima, okolnosti i svrhe obrade.

---

[208] Radna grupa čl. 29 „Smernice o proceni uticaja u vezi sa zaštitom podataka i utvrđivanje da li obrada podataka može „verovatno prouzrokovati visok rizik" u smislu Uredbe 2016/679", Datenschutzgruppe Art. 29 „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 04.04.2017., zuletzt überarbeitet am 04.10.2017., 17/DE, WP 248 Rev. 01, str. 4, 5, 6, 7, 8.

PRIMERI PROMENE RIZIKA
Upotreba novih tehnologija, promena svrhe obrade podataka, obrada većeg broja podataka, upotreba drugih kategorija podataka.

Procena uticaja u vezi sa zaštitom podataka ne mora da se sprovodi za već odobrene postupke obrade podataka. Ovo se odnosi na situacije bazirane na čl. 20 Direktive 95/46/EZ tzv. *predhodne kontrole*, koje je ispitao nadzorni organ za zaštitu podataka. Međutim, ukoliko su se okolnosti *promenile* (u pogledu obima, svrhe, tehničkih i organizacionih mera itd.), iako postoji odobrenje nadzornog organa za zaštitu podataka, neophodno je ponovo sprovesti procenu.

Prema potrebi rukovalac sprovodi preispitivanje kako bi procenio da li je obrada sprovedena u skladu sa procenom uticaja u vezi sa zaštitom podataka barem onda kada postoji promena u visini rizika koji predstavljaju postupci obrade (čl. 35 st. 11 OUZP).

Procenu uticaja u vezi sa zaštitom podataka treba redovno kontrolisati i u definisanim vremenskim periodima ponovno sprovoditi.

Sama procena treba da se obavi *pre* nameravane obrade podataka, još u stadijumu *razvoja koncepta obrade podataka*. Tokom *svih faza projekta* treba konstantno pratiti promene u riziku po pojedince. U toku samog projekta je moguće da se u nekoj fazi pojavi potreba za *ponavljanjem* procene posledica po pojedince, pošto se pojavi visok rizik, koji bi mogao biti smanjen upotrebom odgovarajućih tehničko - organizacionih mera. Stoga sama procena uticaja u vezi sa zaštitom podataka ne predstavlja jednoročnu obavezu za rukovaoca, već *kontinuiran proces*.

Može se desiti u praksi da rukovalac ne sprovede postupak procene uticaja u vezi sa zaštitom podataka, iako postoji visok rizik u pogledu obrade podataka. U tom slučaju rukovalac mora da *obrazloži i dokumentuje*, zbog čega nije sproveo procenu i posavetovao se sa ovlašćenim licem za zaštitu podataka.

Evidencija aktivnosti obrade bi po mišljenju Radne grupe čl. 29 trebalo da sadrži procenu rizika za pojedince. To proizlazi iz obaveze rukovaoca da opiše organizacione i tehničke mere (čl. 30 st. 1 g) i čl. 30 st. 2 d) OUZP). U svakom slučaju se preporučuje da *evidencija aktivnosti obrade obuhvati i procenu rizika za svaku obradu*. Na ovaj način se ispunjava i načelo društvene odgovornosti, a u slučaju kontrole od strane nadzornog organa za zaštitu podataka se odmah ukazuje na rizike.

11.3. Kriterijumi za sprovođenje procene uticaja u vezi sa zaštitom podataka

Pri proceni uticaja u vezi sa zaštitom podataka treba posebno obratiti pažnju na sledeće kriterijume:

- ✓ *Procenu ili rangiranje prilikom pravljenja profila* i prognoza baziranih na ličnim aspektima pojedinaca kao što su učinak na poslu, ekonomsko stanje, zdravlje, lični afiniteti ili interesi, pouzdanost ili ponašanje, lokacija ili kretanje.

PRIMER
Financijska institucija koja proverava svoje klijente u bazi podataka o kreditnoj sposobnosti, u postupku suzbijanja pranja novca i finansiranja terorizma ili u bazi podataka o prevarama; biotehnološko preduzeće koje nudi kupcima genetska testiranja radi procene i predviđanja bolesti/zdravstvenih rizika ili preduzeće koje izrađuje profile ponašanja i marketinške profile bazirane na korišćenju njihove internet stranice.

- ✓ *Automatsko donošenje odluka* sa pravnim ili sličnim značajnim posledicama: obrada čiji je cilj donošenje odluka o pojedincima, koje proizvode pravna dejstva za pojedince ili na sličan način značajno utiču na pojedinca (čl. 35. st. 3. a) OUZP). Obrada podataka može dovesti do isključivanja ili diskriminacije pojedinaca. Obrada podataka čiji je dejstvo na pojedince neznatano ili nikakvo, ne odgovara ovom specifičnom kriterijumu.
- ✓ *Sistematsko praćenje:* obrada koja se koristi za posmatranje, praćenje ili kontrolu pojedinaca, uključujući podatke prikupljene putem mreža ili na osnovu „sistematskog praćenja javno dostupnog područja" (čl. 35 st. 3 c) OUZP). Ova vrsta praćenja je jedan od kriterijuma jer se podaci o ličnosti mogu prikupljati u situacijama u kojima pojedinci nisu svesni ko prikuplja njihove podatke i u koje svrhe će se ti podaci upotrebiti. Osim toga pojedinci možda neće moći da izbegnu takvu obradu na javnim (ili javno dostupnim) mestima (npr. upotreba dronova u marketinške svrhe).
- ✓ *Osetljivi podaci ili podaci vrlo lične prirode*: tu spadaju posebne kategorije ličnih podataka, u smislu čl. 9 OUZP (npr. informacije o političkim mišljenjima pojedinaca), kao i lične podatke koji se odnose na krivične presude ili krivična dela, u smislu čl. 10 OUZP.

PRIMERI
Opšta bolnica koja čuva medicinsku dokumentaciju pacijenata ili privatni detektiv koji čuva pojedinosti o prestupnicima. Osim onoga što nije obuhvaćeno OUZP, za neke kategorije podataka može se smatrati da povećavaju mogući rizik za prava i slobode pojedinaca. Ti lični podaci smatraju se osetljivim jer su povezani sa kućnim i privatnim aktivnostima (poput elektronske komunikacije čija poverljivost mora da bude zaštićena) ili zato što utiču na ostvarivanje osnovnih prava (poput podataka o lokaciji čije prikupljanje dovodi u pitanje slobodu kretanja) ili zato što njihova povreda podrazumeva ozbiljne posledice za svakodnevni život pojedinaca (poput finansijskih podataka koji mogu biti upotrebljeni za prevaru u platnom prometu). U tom pogledu je od značaja da li je pojedinac te podatke već javno objavio ili je to uradila treća strana. Činjenica da su lični podaci javno dostupni može se smatrati faktorom u proceni ako se očekivalo dalje korišćenje tih podataka u određene svrhe. Taj kriterijum može obuhvatati i podatke poput ličnih dokumenata, e-mejlove, dnevnike, beleške sa e-čitača na kojima se mogu praviti beleške sa vrlo ličnim informacijama.

- ✓ *Obrada podataka u velikom obimu:* u OUZP nije određeno šta obuhvata pojam „obimno".

- ✓ Preporučuje se da se, pri utvrđivanju da li je obrada obimna, uzmu u obzir sledeći faktori (U.t.r. 91 OUZP):
- ✓ broj uključenih pojedinaca, kao određeni broj ili udeo relevantnog stanovništva;
- ✓ količina podataka i/ili niz različitih podataka koji se obrađuju;
- ✓ trajanje ili stalnost postupka obrade podataka;
- ✓ geografski obim aktivnosti obrade.
- ✓ *Upoređivanje ili kombinovanje podataka*, npr. oni koji potiču iz dva postupka obrade ili iz više njih, a koji su sprovedeni u različite svrhe i/ili koje su sproveli različiti rukovaoci na način koji može prevazići razumna očekivanja pojedinaca.
- ✓ *Podaci koji se odnose na zaštićene ili osetljive pojedince* (U.t.r. 75 OUZP): obrada ove vrste podataka predstavlja kriterijum zbog velike neravnoteže moći između pojedinaca i rukovaoca, što znači da pojedinci ne mogu jednostavno dati pristanak ili uložiti prigovor na dalju obradu podataka ili ostvarivati svoja prava. Zaštićeni ili osetljivi pojedinci mogu biti deca (smatra se da ne mogu svesno i promišljeno da daju pristanak ili da se usprotive obradi podataka), zaposleni, kategorije stanovništva koje zahtevaju posebnu zaštitu (osobe sa duševnim smetnjama, tražioci azila ili starije osobe, pacijenti itd.). Time su obuhvaćene i situacije u kojima se može utvrditi neravnoteža između položaja pojedinaca i rukovaoca.
- ✓ *Inovativna upotreba ili primena novih tehnoloških ili organizacionih rešenja*, poput kombinovanja otisaka prstiju i prepoznavanja lica radi poboljšane kontrole fizičkog pristupa itd. Iz OUZP (čl. 35 st. 1 i U.t.r. 89 i 91 OUZP) proizlazi da upotreba nove tehnologije, definisane u skladu sa odgovarajućim aktuelnim stanjem tehnike (U.t.r. 91 OUZP) može dovesti do neophodnog sprovođenja procene uticaja u vezi sa zaštitom podataka. To je zato što upotreba takve tehnologije može obuhvatiti inovativne oblike prikupljanja i upotrebe podataka sa mogućim visokim rizikom po prava i slobode pojedinaca. Konačno, lične i društvene posledice implementacije nove tehnologije su teško predvidive. Procena posledica uticaja u vezi sa zaštitom podataka može da pomogne rukovaocu u razumevanju rizika i postupanju sa njima. Npr. određene aplikacije „internet stvari" mogu znatno uticati na svakodnevni život i privatnost pojedinaca; stoga je neophodno sprovesti procenu uticaja u vezi sa zaštitom podataka.
- ✓ Slučajevi u kojoj sama obrada podataka *sprečava pojedince u ostvarivanju prava ili upotrebi usluga odnosno sprovođenju ugovora* (čl. 22. i U.t.r. 91 OUZP). To uključuje i postupke obrade u kojima se pojedincima dopušta, menja ili odbija pristup pojedinoj usluzi ili sklapanje ugovora. Primer za ovo je banka koja proverava klijente u referentnoj bazi podataka o kreditnoj sposobnosti (provera boniteta) pri odlučivanju o dodeli kredita.

Ukoliko postupak obrade ispuni *dva kriterijuma* od navedenih, rukovalac mora sprovesti procenu uticaja u vezi sa zaštitom podataka. Što više kriterijuma ispunjava određena obrada podataka, to je potrebnije sprovesti procenu uticaja u vezi sa zaštitom

podataka, nezavisno od toga koje su zaštitne mere predviđene.[209] U nekim situacijama će rukovalac biti u obavezi da sprovede procenu, iako je ispunjen samo jedan kriterijum.[210]

11.4. Primeri obrada gde verovatno postoji neophodnost sprovođenja procene uticaja u vezi sa zaštitom podataka

Primeri obrade	*Mogući relevantni kriterijumi*
Bolnica koja obrađuje genetske i zdravstvene podatke svojih pacijenata (bolnički informacioni sistem).	- Tajni podaci ili podaci vrlo lične prirode. - Podaci koji se odnose na posebno zaštićene pojedince (invalide, trudnice itd.). - Obimne obrade podataka.
Upotreba sistema nadzornih kamera za praćenje ponašanja vozača na autoputevima. Rukovalac namerava da upotrebi sistem pametne video analize za identifikovanje automobila i automatsko prepoznavanje registarskih tablica.	- Sistematsko praćenje. - Inovativna upotreba ili primena tehnoloških ili organizacionih rešenja.
Preduzeće sistematski prati aktivnosti svojih zaposlenih, uključujući praćenje računara, aktivnost na internetu itd.	- Sistematsko praćenje. - Podaci koji se odnose na posebno zaštićene pojedince (invalide, trudnice itd.).
Prikupljanje javno dostupnih podataka sa društvenih mreža radi izrade profila.	- Procena ili rangiranje. - Obimna obrada podataka. - Upoređivanje ili kombinovanje podataka. - Osetljivi podaci ili podaci vrlo lične prirode. - Tajni podaci ili podaci vrlo lične prirode.
Institucija koja uspostavlja bazu podataka kreditnog rejtinga ili prevara na nacionalnom nivou.	- Procena ili rangiranje. - Automatsko donošenje odluka sa pravnim ili sličnim značajnim dejstvom. - Sprečavanje pojedinca u ostvarivanju prava, korišćenju usluge ili sprovođenju ugovora. - Tajni podaci ili podaci vrlo lične prirode.
U svrhu arhiviranja se čuvaju pseudonimizovani podaci o ličnosti koji se odnose na zaštićene pojedince u okviru istraživačkih projekata ili kliničkih ispitivanja.	- Tajni podaci - Podaci zaštićenih pojedinca (invalida, trudnica itd.). - Sprečavanje pojedinaca u ostvarivanju prava, korišćenju usluga ili sprovođenju ugovora.

[209] Primeri metoda spovođenja procene posledica po pojedince: 1) DE: Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung, 2016, https:// www. datenschutzzentrum. de/ uploads/ sdm/SDM-Methode_V_1_1.pdf, 2) ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014. https:// www.agpd. es/ portalwebAGPD/ canaldocumentacion/ publicaciones/common/Guias/Guia_EIPD.pdf, 3) FR: Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015., https://www.cnil.fr/fr/node/15798, 4) UK: Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014., https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

[210] *Ibidem*, str. 10, 11, 12.

11.5. Primeri obrada gde verovatno ne postoji neophodnost sprovođenja procene uticaja u vezi sa zaštitom podataka[211]

Primeri obrade	*Mogući relevantni kriterijumi*
Obrada „ličnih podataka pacijenata ili klijenata pojedinih lekara, zdravstvenih radnika ili advokata" (U.t.r. 91 OUZP).	- Tajni podaci ili podaci vrlo lične prirode. - Podaci zaštićenih pojedinca (invalida, trudnica itd.).
Časopis na internetu čiji urednici koriste spisak adresa za slanje dnevnih novosti svojim pretplatnicima.	- Obrada podataka u velikom obimu.
Internet stranica e-trgovine koja prikazuje reklame za delove oldtajmera, što obuhvata i izradu profila na osnovu pregleda ili kupovine na internet stranici prodavca.	- Procena ili rangiranje.

Inače procenu uticaja u vezi sa zaštitom podataka *nije neophodno sprovesti*:[212]

- ✓ Kada se radi o obradi koja verovatno ne nosi sa sobom visok rizik ili
- ✓ Kada je već slična procena sprovendena ili
- ✓ Kada je obrada odobrena pre 25. maja 2018. godine ili
- ✓ Kada je izričito zakonski isključena (čl. 6 st. 1 c) OUZP) ili
- ✓ Nije potrebna za sprovođenje zadataka u javnom interesu ili vršenje vlasti (čl. 6 st. 1 e) OUZP) ili
- ✓ Se radi o "beloj listi" za koju procena posledica uticaja u vezi sa zaštitom podataka nije neophodna (čl. 35 st. 5 OUZP).[213]

11.6. Dužnosti u okviru postupka procene uticaja u vezi sa zaštitom podataka

Obavezu sprovođenja procene uticaja u vezi sa zaštitom podataka imaju u prvom redu *rukovaoci*. Rukovalac se mora *posavetovati sa ovlašćenim licem za zaštitu podataka*, ukoliko postoji ova funkcija u organizaciji (čl. 35 st. 2 OUZP). Ovaj savet treba dokumentovati. Ovlašćeno lice za zaštitu podataka je u obavezi da nadzire sam postupak sprovođenja procene uticaja u vezi sa zaštitom podataka (čl. 39 st. 1 c) OUZP).

---

[211] *Ibidem*, str. 13, 14.

[212] *Ibidem*, str. 15.

[213] Crne liste Nemačka, kada se mora sprovesti procena posledica po pojedince https://www.datenschutz-notizen.de/deutsche-aufsichtsbehoerden-legen-blacklist-vor-0920586/;

Bele liste Austrija, kada se ne mora sprovoditi procena posledica po pojedince. http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.html.

Ukoliko obradu podataka sprovodi u potpunosti ili delimično *obrađivač*, on mora da *pomogne* rukovaocu u sprovođenju procene uticaja u vezi sa zaštitom podataka i stavi na raspolaganje neophodne informacije (čl. 28 st. 3 f) OUZP).

Svaki postupak procene uticaja u vezi sa zaštitom podataka treba da sadrži (čl. 35 st.7 OUZP):

- ✓ Opis postupaka obrade podataka i svrhe, ako je potrebno pretežniji interes;
- ✓ Procenu neophodnosti i proporcionalnosti obrade podataka u odnosu na svrhu;
- ✓ Procenu rizika po prava i slobode pojedinaca;
- ✓ Mere za umanjenje rizika;
- ✓ Dokaze preduzetih mera.

Rukovalac može, ako je neophodno da zatraži *mišljenje o nameravanoj obradi od pojedinca* ili njegovog zastupnika (čl. 35 st. 9 OUZP). Bitno je naglasiti da se u ovom slučaju ne radi o pribavljanju saglasnosti pojedinaca, već izražavanju mišljenja. Ovo mišljenje može biti izraženo u vidu anketa, studija, upita interesnih zajednica poput sindikata, radnih saveta itd.

Ukoliko mišljenje odstupa od stava i odluke rukovaoca, razloge treba dokumentovati. Takođe ako se uopšte ne zatraži mišljenje potrebno je dokumentovati razloge za to (npr. isuviše veliki napor, neproporcionalnost, povreda poslovne tajne itd.).

Rukovalac mora da *konsultuje nadzorni organ za zaštitu podataka*, ukoliko nije preduzeo adekvatne mere za umanjenje rizika, a rizik po sprovedenoj proceni posledica po pojedince je i dalje visok (čl. 36 st. 1 OUZP). To se odnosi dakle samo na one slučajeve kada rukovalac nije uspeo da umanji rizike po sprovedenoj proceni uticaja u vezi sa zaštitom podataka. U slučaju da je visok rizik smanjen, rukovalac nema obavezu da konsultuje nadzorni organ za zaštitu podataka.

Osim toga rukovalac *može* biti u obavezi da konsultuje nadzorni organ za zaštitu podataka, ukoliko je to predviđeno pravom države članice EU. Tom prilikom nadzorni organ za zaštitu podataka daje predhodno odobrenje za obradu podataka, koju obavlja rukovalac u svrhu obavljanja zadataka u javnom interesu, uključujući i obradu u vezi sa socijalnom zaštitom i javnim zdravljem (čl. 36 st. 5 OUZP).[214]

Sprovodeći procenu uticaja u vezi sa zaštitom podataka rukovalac mora da uzme u obzir sledeće korake:

- ✓ integraciju u postojeće postupke oblikovanja, razvoja, promene, utvrđivanja rizika i operativnog preispitivanja u skladu sa unutrašnjim procesima, kontekstom i kulturom;
- ✓ uključivanje zainteresovanih strana, čija je odgovornost jasno definisana

[214] *Ibidem*, str. 18, 19, 23, 24, 25.

(rukovalac, ovlašćeno lice za zaštitu podataka, pojedinci ili njihovi predstavnici, poslovni subjekti, tehničke službe, obrađivači, ekspert za informacionu bezbednost itd.);

- ✓ ako je potrebno dostaviti izveštaj o proceni uticaja u vezi sa zaštitom podataka nadzornom organu za zaštitu podataka;
- ✓ konsultovanje nadzornog organa za zaštitu podataka, ukoliko nisu preduzete mere za umanjenje visokog rizika;
- ✓ ispitivanje u redovnim razmacima procene uticaja u vezi sa zaštitom podataka i procena obrade podataka, barem onda kada se promeni rizik za određenu aktivnost obrade;
- ✓ dokumentovanje donešene odluke o proceni uticaja u vezi sa zaštitom podataka.

11.7. Kontrolna pitanja postupka procene uticaja u vezi sa zaštitom podataka

- o *Procena treba da sadrži sistematski opis obrade* (član 35. st. 7. a) OUZP):
  - o u obzir su treba uzeti prirodu, obim, kontekst i svrhe obrade (U.t.r. 90 OUZP);
  - o treba zabeležiiti podatke o ličnosti, primaoce i rok čuvanja podataka o ličnosti;
  - o treba navesti funkcionalni opis postupka obrade;
  - o treba proceniti sredstva od kojih zavise lični podaci (oprema, hardver, softver, mreže, osobe, dokumenti u papirnom obliku ili kanali za slanje dokumenata u papirnom obliku);
  - o treba uzeti u obzir i usklađenost sa odobrenim kodeksima ponašanja (čl. 35. st. 8 OUZP);
- o *Procena neophodnosti i proporcionalnost* (čl. 35. st. 7 b) OUZP):
  - o treba predvideti mere za usklađivanje sa OUZP (čl. 35. st. 7 d) OUZP i U.t.r. 90 OUZP), uzimajući u obzir mere koje doprinose proporcionalnosti i neophodnosti obrade na osnovu:
  - o posebnih, nedvosmislenih i zakonitih svrha (čl. 5 st. 1 b) OUZP);
  - o zakonitosti obrade (čl. 6 OUZP);
  - o proporcionalnost i neophodnost podataka, ograničenih na ono što je neophodno za obradu (čl. 5 st. 1 c) OUZP);
  - o ograničeno trajanja čuvanja podataka (čl. 5 st. 1 e) OUZP);
- o *Mere koje doprinose pravima pojedinaca*:
  - o informacije pružene pojedincu (čl. 12, 13 i 14 OUZP);
  - o pravo na informaciju o obradi i prenosivost podataka (čl. 15 i 20 OUZP)
  - o pravo na ispravku i brisanje podataka (čl. 16, 17 i 19 OUZP);
  - o pravo na prigovor i ograničavanje obrade podataka (čl. 18, 19 i 21 OUZP);
  - o odnos sa obrađivačima (čl. 28 OUZP);
  - o zaštitne mere koje se odnose na međunarodni prenos podataka (poglavlje V.);

- prethodno konsultovanje nadzornog organa za zaštitu podataka (čl. 36 OUZP).

o *Kontrolisanje rizika po prava i slobode pojedinaca* (čl. 35. st. 7 c) OUZP):
- treba proceniti uzrok, vrstu, posebnost i ozbiljnost rizika (U.t.r. 84 OUZP) ili detaljno za svaki rizik (neovlašćeni pristup, neželjene izmene i gubitak podataka) izvršiti procenu rizika iz perspektive pojedinaca:
- treba uzeti u obzir izvore rizika (U.t.r. 90 OUZP);
- treba utvrditi moguće posledice po prava i slobode pojedinaca između ostalog u slučaju neovlašćenog pristupa, neželjene izmene i gubitka podataka;
- treba utvrditi pretnje koje mogu dovesti do neovlašćenog pristupa, neželjene izmene i nestanka podataka;
- treba proceniti verovatnoću i ozbiljnost rizika (U.t.r. 90 OUZP);
- treba proceniti mere za uklanjanje ili umanjenje rizika (čl. 35 st. 7 d) i U.t.r. 90 OUZP);

o *Uključenost zainteresovanih strana*:
- zatražen je savet ovlašćenog lica za zaštitu podataka (čl. 35 st. 2 OUZP);
- prema potrebi zatražena mišljenja pojedinaca ili njihovih predstavnika (čl. 35. st. 9 OUZP).[215]

[215] *Ibidem*, str. 28, 29.

12. OBAVEŠTAVANJE O POVREDI BEZBEDNOSTI PODATAKA O LIČNOSTI „Data Breach“ (čl. 33 i 34 OUZP)

12.1. Obaveštavanje nadzornog organa o povredi bezbednosti podataka o ličnosti (čl. 33 OUZP)

OUZP zahteva od rukovaoca i obrađivača da koriste odgovarajuće tehničke i organizacione mera, kako bi osigurali odgovarajuću bezbednost ličnih podataka (čl. 32 OUZP). To podrazumeva zaštitu od neovlašćene ili nezakonite obrade i od slučajnog gubitka, uništenja ili šteta. Od rukovaoca i obrađivača se dakle zahteva da imaju odgovarajuće tehničke i organizacione mere kako bi osigurali nivo bezbednosti koji odgovara riziku koji se odnosi na podatke o ličnosti koji se obrađuju. Pritom potrebno je uzeti u obzir stanje tehnike, troškove implementacije i prirodu, obim, kontekst i svrhu obrade, kao i rizik od promene, verovatnoću nastupanja posledica po prava i slobode fizičkih lica.

OUZP zahteva da se za svu odgovarajuću tehničku zaštitu uspostave organizacione mere kako bi se u najkraćem roku utvrdilo da li je došlo do povrede bezbednosti i ustanovilo da li je neophodna obaveza obaveštenja. Čl. 32 OUZP jasno stavlja do znanja da rukovalac i obrađivač treba da imaju odgovarajuće tehničke i organizacione mere u cilju osiguranja odgovarajućeg nivoa bezbednosti ličnih podataka što podrazumeva *sposobnost detekcije, adresiranja i blagovremenog prijavljivanja* povreda bezbednosti.

U pogledu organizacionih mera zaštite podrazumeva se postojanje *politike bezbednosti podataka*. Ovim pravilom bi trebalo regulisati sprečavanje povreda bezbednosti podataka, kao i pravovremenu reakciju ukoliko se povreda dogodi.

OUZP definiše *”povredu bezbednosti podataka o ličnosti”* (čl. 4 tč. 12):

*”*Kršenje bezbednosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima o ličnosti koji su preneti, uskladišteni ili na drugi način obrađivani.”.

Pod *”uništavanjem*” ličnih podataka podrazumeva se da podaci više ne postoje ili više ne postoje u obliku koji je od bilo kakve koristi rukovaocu.

” Šteta” podrazumeva da su lični podaci izmenjeni, zloupotrebljeni ili nisu više kompletni.

” Gubitak” ličnih podataka predpostavlja da podaci i dalje postoje, ali je rukovalac izgubio kontrolu ili pristup nad njima, ili podatke više ne poseduje.

” Neovlašćena ili nezakonita obrada” može obuhvatati otkrivanje ličnih podataka primaocima ili pristup podacima licima koji nisu ovlašćeni da primaju ili pristupe podacima ili bilo koji drugi oblik obrade koji krši OUZP.

PRIMERI GUBITKA PODATAKA
Uređaj koji sadrži kopiju baze podataka klijenta, koji je izgubljen ili ukraden. Primer gubitka podataka može biti gde je jedina kopija skupa ličnih podataka bila kriptovana od strane ransomware (zlonamerni softver koji šifrira podatke rukovaoca dok se ne plati otkup) ili je rukovalac šifrovao koristeći ključ koji više ne poseduje.

Povreda bezbednosti podataka je vrsta bezbednosnog incidenta. Shodno definiciji (čl. 4 t. 12 OUZP) povreda bezbednosti postoji samo ako *postoji povreda bezbednosti podataka o ličnosti.* Posledica povrede bezbednosti podataka je da rukovalac neće biti u stanju da osigura poštovanje principa, koji se odnose na obradu ličnih podataka (čl. 5 OUZP).

Razliku između bezbednosnog incidenta i povrede bezbednosti ličnih podataka je u tome što su sve povrede ličnih podataka bezbednosni incidenti, dok *nisu svi bezbednosnosni incidenti nužno povreda ličnih podataka*.

Povrede bezbednosti mogu biti *kategorizovane* prema poznatim principima bezbednosti informacija:

- ✓ *"povreda poverljivosti"* - ako postoji neovlašćeno ili slučajno otkrivanje ili pristup ličnim podacima.
- ✓ *"povreda integriteta"* - ako postoji neovlašćena ili slučajna promena ličnih podataka.
- ✓ *"povreda dostupnosti"* - ako postoji slučajan ili neovlašćen gubitak pristupa ili uništavanje ličnih podataka.

Treba napomenuti da, u zavisnosti od okolnosti, povreda bezbednosti može da se odnosi na poverljivost, integritet i dostupnost ličnih podataka istovremeno, kao i svaku njihovu kombinaciju. Kada lični podaci nisu dostupni zbog planiranog održavanja sistema, ovo ne predstavlja povredu bezbednosti.[216]

PRIMERI GUBITAK DOSTUPNOST PODATAKA
Za bolnice, ako kritični medicinski podaci o pacijentima nisu dostupni, čak i privremeno, to bi moglo predstavljati rizik za prava i slobode pojedinaca. Npr. operacije mogu biti otkazane, a pacijenti ugroženi. U slučaju da sistem nekoj medijskoj kompaniji nije dostupan nekoliko sati (npr. nestanak električne energije), što ovo preduzeće onemogućava u slanju biltena svojim pretplatnicima, malo je verovatno da će predstavljati rizik za pojedinace.

Od značaja je da iako gubitak dostupnosti sistema rukovaoca samo privremeni i možda neće uticati na pojedince, važno je da *rukovalac razmotri sve moguće posledice povrede bezbednosti*, jer obaveza obaveštavanja može postojati i iz drugih razloga.

---

[216] Radna grupa član 29, *Smernice za obaveštavanje o povredi bezbednosti podataka o ličnosti po Uredbi 2016/679*, usvojeno 03.10.2017, izmenjeno i dopunjeno 06.02.2018, str. 6, 7, 8. The Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 03.10.2017, As last Revised and Adopted on 06.10.2018., 18/EN, WP250rev.01.

PRIMER PRIVREMENOG GUBITKA DOSTUPNOSTI PODATAKA
Infekcija putem ransomware-a (zlonamerni softver koji šifrira podatke rukovaoca dok se ne plati otkup) može dovesti do privremenog gubitka dostupnosti ako se podaci mogu vratiti iz rezervne kopije.

12.1.1. Obaveza obaveštavanja nadzornog organa i procena rizika

Povreda bezbednosti podataka može imati kao posledicu različiti spektar negativnih efekata po pojedince, što može dovesti do fizičke, materijalne ili nematerijalne štete.

PRIMERI POSLEDICA PO POJEDINCE ZBOG POVREDE BEZBEDNOSTI PODATAKA O LIČNOSTI
Gubitak kontrole nad ličnim podacima, ograničavanje prava pojedinaca, diskriminacija, krađa identiteta ili prevara, finansijski gubitak, neovlašćeno korišćenje pseudonimizovanih podataka, gubitak reputacije i gubitak poverljivosti ličnih podataka zaštićenih profesionalnom tajnom. Osim toga povreda bezbednosti podataka o ličnosti može uključiti bilo koji drugi značajan ekonomski ili socijalni gubitak za pojedince. Kada se povreda bezbednosti odnosi lične podatke koji otkrivaju rasno ili etničko poreklo, političko mišljenje, veroispovest ili filozofska uverenja ili članstvo u sindikatu ili uključuju genetske podatke, podatke o zdravlju ili podatke o seksualnom životu ili podatke o krivičnim presudama i krivičnim delima, takva šteta treba smatrati verovatnom da se desi.

OUZP ne zahteva od rukovaoca da obaveštava o povreda bezbednosti nadležni nadzorni organ, ako je malo verovatno da će to dovesti do rizika i štetnih efekata za pojedince. Potrebno je da postoji *rizik po pojedince*.

U slučajevima gde postoji verovatno visok rizik od nastanka neželjenih posledica, OUZP zahteva od rukovaoca da obavesti o povredi bezbednosti pogođene osobe čim to bude razumno izvodljivo.

Rukovalac je u obavezi da (čl. 33 st. 1 OUZP):
''U slučaju povrede bezbednosti podataka o ličnosti *bez nepotrebnog odlaganja* i,ukoliko je moguće, *najkasnije 72 sata nakon saznanja* o toj povredi zvanično obaveštava nadzorni organ nadležan u skladu sa članom 55, osim u slučaju da nije verovatno da će povredom bezbednosti podataka o ličnosti biti ugrožena prava i slobode fizičkih lica. Ako zvanično obaveštavanje nije izvršeno u roku 72 sata, navodi se *obrazloženje za kašnjenje*.''.

Obavezu obaveštavanja nadzornog organa detaljnije objašnjava (U.t.r. 87 OUZP):
''treba proveriti da li su preduzete sve odgovarajuće mere tehnološke zaštite i organizacione mere da bi se odmah utvrdilo da li je došlo do povrede podataka o ličnosti i da bi se odmah obavestio nadzorni organ i lice na koje se podaci odnose. Treba utvrditi činjenicu da li je obaveštenje dato bez nepotrebnog odlaganja posebno

uzimajući u obzir prirodu i ozbiljnost povrede podataka o ličnosti i njene posledice i negativne efekte za lice na koje se podaci odnose. Takvo obaveštenje može da dovede do intervencije nadzornog organa u skladu sa njegovim zadacima i ovlašćenjima propisanim ovom uredbom.''.

OUZP zahteva da, u slučaju povrede bezbednosti rukovalac obavesti o povredi bezbednosti bez nepotrebnog odlaganja, a najkasnije u roku 72 sata nakon što je *postao svestan povrede bezbednosti* (čl. 33 st. 2 OUZP). Pravo je pitanje kada se može smatrati da je rukovalac *''* svestan*''* da se dogodila povreda bezbednosti. Radna grupa čl. 29 smatra da rukovalac postao *'*svestan*''* *kada se sa razumnim stepenom sigurnosti može tvrditi da je došlo do bezbedonosnog incidenta koji je doveo do kompromitacije ličnih podataka*.[217]

Kao što je već navedeno OUZP zahteva od rukovaoca da sprovede sve odgovarajuće tehničke zaštite i organizacione mere kako bi utvrdio da li je došlo do povrede i da bez odlaganja obavesti nadzorni organ i pojedince. Ovo treba tumačiti kao obavezu rukovaoca da osigura *blagovremenu reakciju ali i svest od svim povredama bezbednosti* kako bi mogao da preduzme odgovarajuće mere.

Kada se tačno, rukovalac može smatrati da je *''* svestan*''* određene povrede bezbednosti zavisiće od okolnosti specifične povrede. Nekada će od samog početka biti jasno da je došlo do povrede bezbednosti, dok u drugim slučajevima može potrajati neko vreme da se utvrdi da li su lični podaci kompromitovani. Stoga bi fokus trebalo da bude na brzoj akciji ispitivanja incidenta kako bi se utvrdilo da li su lični podaci kompromitovani, i ako jesu trebalo bi preduzeti popravne radnje i sprovesti obaveštenje ako je potrebno.

O samoj povredi bezbednosti rukovalac može biti obavešten od strane pojedinca, medija ili nekog drugog izvora, ali i kada sam otkrije bezbedonosni incident. Od svih ovih informacija rukovalac treba da preduzme kratku istragu kako bi ustanovio, da li se bezbednosnosni incident dogodio. U ovom kratkom periodu se rukovalac *ne može smatrati ''svesnim''* . Međutim, očekuje se da se početna istraga što pre započne i utvrdi razuman nivo verovatnoće da li je došlo do povrede bezbednosti. Potom sledi detaljnija istraga.

Kada rukovalac postane svestan, obaveštenje o povredi bezbednosti mora biti obavljeno bez nepotrebnog odlaganja najkasnije u roku od 72 sata. Tokom ovog perioda, rukovalac bi trebalo da proceni verovatnoću nastupanja rizika po pojedinaca kako bi utvrdio da li treba pokrenut proces obaveštavanja, kao proces i aktivnosti koje su potrebne za rešavanje povreda bezbednosti.

Rukovalac može već imati *inicijalnu procenu potencijalnog rizika* koji bi mogao biti rezultat povreda bezbednosti kao *deo procene uticaja u vezi sa zaštitom podataka***.** Procena uticaja u vezi sa zaštitom podataka *može biti više generalizovana u* odnosu na specifične okolnosti bilo koje stvarne povrede, tako da u svakom slučaju treba napraviti dodatnu procenu uzimajući u obzir te okolnosti.

Preporučuje se da kada se otkrije povreda bezbednosti podataka o ličnosti, da se ova *povreda prijavi najvišem menadzmentu i odgovarajućem nivou upravljanja.*

[217] *Ibidem*, str. 9, 10.

Pravovremene mere zaštite i mehanizmi izveštavanja mogu biti detaljno opisane u *planovima za odgovor na incidentne situacije* rukovaoca (kao deo politike o bezbednosti podataka). Ovo će pomoći rukovaocu da efikasno planira i utvrdi ko ima operativnu odgovornost u organizaciji za upravljanje povredama bezbednosti kao i postupak eskalacije incidenta.

12.1.2. Primeri kada obaveštenje nije potrebno

Povrede bezbednosti koje*" neće verovatno da će dovesti do rizika za prava i slobode fizičkih lica"* ne zahtevaju obaveštenje nadležnom organu. U slučaju da *obaveštenje o povredi bezbednosti podataka o ličnosti nije potrebno* ono nije potrebno ni za obaveze rukovaoca shodno čl. 33 prema nadzornom organu kao ni za obaveze shodno čl. 34 OUZP prema pojedincima.

PRIMER KADA OBAVEŠTENJE NIJE POTREBNO
Lični podaci su već javno dostupni i otkrivanje takvih podataka ne predstavlja potencijalni rizik za pojedinca.

PRIMER KADA OBAVEŠTENJE NIJE POTREBNO
Povreda bezbednosti ličnih podataka koji su šifrirani sa najsavremenijim algoritmom predstavlja povredu bezbednosti ličnih podataka, te stoga mora doći do obaveštenja. Međutim, ako poverljivost ključa nije ugrožena i ključ je bio generisan tako da se ne može utvrditi raspoloživim tehničkim sredstvima od strane lica koja nemaju ovlašćenja pristupa, tada su podaci u principu nerazumljivi. Stoga, je verovatnoća da će povreda bezbednosti podataka o ličnosti negativno uticati na pojedince mala, pa ne bi trebalo obaveštavati pojedince. Treba imati u vidu da čak i kada su podaci šifrirani, gubitak ili promena može imati negativne posledice za pojedince gde rukovalac nema adekvatne sigurnosne kopije. U tom slučaju biće potrebno sprovesti obaveštenje pojedincima, iako sami podaci podležu odgovarajućim merama šifriranja.

PRIMER KADA JE OBAVEŠTENJE POTREBNO
Ako postoji povreda bezbednosti i ne postoje rezervne kopije ličnih podataka, to bi moglo predstavljati rizike pojedinca i stoga se zahteva obaveštenje.

PRIMER KADA JE OBAVEŠTENJE POTREBNO
Kada se izgube podaci koji su šifrirani, čak i ako postoji rezervna kopija ličnih podataka, to može i dalje biti povreda bezbednosti podataka od ličnost, zavisno od dužine vremena potrebnog za vraćanje podataka iz rezervnih kopija i efekta nedostatka dostupnosti za pojedince. Važan faktor bezbednosti je "sposobnost blagovremenog ponovnog uspostavljanja dostupnosti podataka o ličnosti i pristupa njima u slučaju fizičkog ili tehničkog incidenta" (čl. 32 st. 1) c) OUZP).

PRIMER KADA OBAVEŠTENJE NIJE POTREBNO
Povreda bezbednosti koja ne zahteva obaveštenje nadzornom organu biće gubitak šifrovanog mobilnog uređaja, koji koristi rukovalac i njegovo osoblje, ako je ključ za šifrovanje ostao u posedu rukovaoca. Osim toga preduslov je da izgubljeni podaci o ličnosti postoje i na sigurnosnim kopijama, pa su stoga nepristupačni za napadače. To znači da povreda verovatno neće dovesti do rizika za prava i slobode pojedinaca. Ako kasnije postane očigledno da je ključ za šifrovanje ugrožen ili da je softver za šifrovanje ili algoritam ranjiv, onda će se rizik za prava i slobode fizičkih lica promeniti i stoga će možda biti potrebno obaveštavanje. Stoga, prilikom odabira softvera za šifrovanje rukovalac treba pažljivo da uzme u obzir kvalitet i pravilno sprovođenje ponuđene enkripcije, razume koji nivo zaštite zapravo pruža i da li je to prikladno za predstavljene rizike. Enkripciju takođe mogu smatrati trenutno odgovarajućim standardom za bezbednost podataka. Međutim, ova tehnologija može da zastari za nekoliko godina, što znači da je upitno da li će podaci biti dovoljno zaštićeni određenim postupkom enkripcije.[218]

12.1.3. Način pružanja informacija nadzornom organu i obaveštavanje u fazama

Kada rukovalac obaveštava o povredi bezbednosti podataka nadzorni organ *obaveštenje treba da sadrži* (čl. 33 st. 3 OUZP):

- ✓ opis prirode povrede bezbednosti podataka o ličnosti, ako je moguće sa navedenim kategorijama i približnim brojem lica na koja se podaci odnose, kao i kategorijama i približnim brojem zbirki evidencija podataka o ličnosti;
- ✓ ime i podatke za kontakt ovlašćenog lica za zaštitu podataka ili druge kontaktne tačke od koje se može dobiti još informacija;
- ✓ opis verovatne posledice povrede bezbednosti podataka o ličnosti;
- ✓ opis mera koje je rukovalac preduzeo ili čije preduzimanje predlaže radi otklanjanja povrede bezbednosti podataka o ličnosti, uključujući prema potrebi i mere za ublažavanje njenih štetnih posledica.

OUZP ne definiše *kategorije subjekata podataka/pojedinaca* (eng. categories of data subjects) kao ni *evidencije kategorija ličnih podataka* (eng. categories of personal data records).

Radna grupa član 29 smatra da se *pod kategorijama subjekata podataka/ pojedinaca* smatraju različiti tipovi pojedinaca čiji lični podaci su pogođeni kršenjem npr. deca i druge ugrožene grupe, osobe sa invaliditetom, zaposleni ili kupci.

Evidencije kategorija ličnih podataka se odnose na različite vrste zapisa koje rukovalac može obraditi, kao što su npr. zdravstveni podaci, podaci o obrazovanju, informacije o socijalnoj zaštiti, finansijski podaci, brojevi bankovnih računa, brojevi pasoša itd.

[218] *Ibidem*, str. 18, 19.

Jedna od svrha obaveštenja o povredi bezbednosti je ograničavanje štete pojedinca (U.t.r. 85 OUZP). Ako tipovi subjekata podataka ili vrste ličnih podataka ukazuju na rizik od posebne štete koja se javlja kao rezultat povreda bezbednosti (npr. krađa identiteta, prevara, finansijski gubitak, pretnja po profesionalnu tajnu), onda je važno da obaveštenje ukazuje na ove kategorije.

Kada precizne informacije nisu dostupne (npr. tačan broj pogođenih pojedinaca/ subjekata podataka) OUZP omogućava približnost u broju pogođenih lica i broja evidencija ličnih podataka. Fokus treba usmeriti na rešavanje negativnih efekata kršenja umesto pružanja preciznih podataka. Zbog toga, kada je došlo do povrede bezbednosti, ali detalji vezani za povredu bezbednosti nisu poznati, omogućeno je *obaveštenje u fazama* (čl. 33 st. 4 OUZP) "Ako nije moguće i u meri u kojoj nije moguće istovremeno pružiti informacije, informacije se mogu dostavljati u delovima, bez nepotrebnog dodatnog odlaganja". Različite vrste povreda (poverljivost, integritet ili dostupnost) mogu zahtevati dodatne informacije koje se trebaju pružiti kako bi se u potpunosti objasnile okolnosti svakog slučaja. OUZP prepoznaje da rukovaoci neće uvek imati sve neophodne informacije u vezi sa povredom bezbednosti u roku od 72 sata nakon što postanu svesni toga, pošto potpuni i sveobuhvatni detalji o incidentu možda nisu uvek dostupni na početku. Zbog toga se dozvoljava obaveštenje u fazama.

Obaveštavanje u fazama je dopušteno pod uslovom da rukovalac navede *razloge za odlaganje* (čl. 33 st. 1 OUZP). Kada rukovalac prvi put obavesti nadzorni organ treba da naznači ako još nema sve potrebne informacije kao i da će kasnije pružiti više detalja.

Suština obaveze obaveštavanja je da podstakne rukovaoce da odmah postupaju ako se dogodi povreda bezbednosti, da pokušaju da spreče povredu, da povrate kompromitovane lične podatke i da potraže odgovarajuće savete od nadzornog organa. U nekim slučajevima biće očigledno da će, zbog prirode povrede i ozbiljnosti rizika, rukovalac morati bez odlaganja da obavesti pogođene pojedince npr: pretnja po krađu identiteta, ako se na internetu otkriju posebne kategorije ličnih podataka.

Koga treba najpre obavestiti u ovakvim slučajevima povreda bezbednosti nije relevantno. Obaveštenje nadzornog organa ne može služiti kao opravdanje za nepoštovanje komunikacije pogođenim pojedincima gde je to potrebno.

Ako je rukovalac obavio inicijalno obaveštenje, preporučuje se da ponovo obavesti nadležni organ ukoliko naknadna istraga otkrije dokaže da je bezbednosni incident uspešno rešen i da nije došlo do povrede bezbednosti podataka o ličnosti. *Ne postoji sankcija* za prijavljivanje incidenta za koje se na kraju ispostavi da se ne radi o povredi bezbednosti podataka o ličnosti.[219]

[219] *Ibidem*, str. 14, 15, 16.

12.2. Obaveštavanje pojedinaca o povredi bezbednosti podataka o ličnosti (čl. 34 OUZP)

Rukovaoci obavezno moraju da obaveste nadležni organ, osim ako je malo verovatno da postoji rizik za prava i slobode pojedinaca zbog povrede bezbednosti. Pored toga, tamo gde postoji *verovatnoća da će nastupiti visok rizik* za prava i slobode pojedinaca kao rezultat bezbednosti, takođe i *pojedinci moraju biti informisani* (čl. 34 st. 1 OUZP). Za razliku od prijavljivanja povrede nadzornom organu gde treba da postoji samo verovatnoća da će nastupiti rizik za pojedince, kod prijavljivanja povrede pojedincima zahteva se *verovatnoća da će nastupiti visok rizik po pojedince*.

I u ovom slučaju se zahteva od rukovaoca da komunikacija o povredi bezbednosti podataka prema pojedincima bude sprovedena "bez nepotrebnog odlaganja", što znači što je pre moguće. Svrha obaveštavanja pojedinaca je da im se omoguće konkretne informacije o koracima koje treba preduzeti da bi se zaštitili od bilo kakvih negativnih posledica povreda bezbednosti podataka o ličnosti.

Prilikom obaveštavanja pojedinaca (čl. 34 st. 2 OUZP) samo obaveštenje treba da bude napisano jasnim i jednostavnim jezikom. U obaveštenju treba da se opiše priroda povrede bezbednosti podataka o ličnosti kao i *informacije o*

- ✓ imenu i kontakt podacima ovlašćenog lica zaštitu podataka ili druge kontaktne tačke;
- ✓ opisu verovatnih posledica povrede bezbednosti podataka o ličnosti; i
- ✓ opisu mera koje je rukovalac preduzeo ili čije preduzimanje predlaže radi otklanjanja povrede bezbednosti podataka o ličnosti, uključujući prema potrebi i mere za ublažavanje njenih štetnih posledica.

Obaveza obaveštenja pojedinaca treba da usledi nakon informisanja nadzornog organa, ukoliko rizik u startu nije bio visok. Rukovalac treba da sprovede savet nadzornog organa o upravljanju kršenjem i smanjivanju uticaja na pojedinca, preduzme mere za rešavanje povreda i ublažavanje mogućih štetnih efekata povrede bezbednosti.

Osim toga rukovalac treba da da specifične savete pojedincima kako bi se zaštitili od mogućih štetnih posledica kršenja, kao što je promena lozinki u slučaju kada su njihovi pristupni podaci ugroženi.

Povreda bezbednosti podataka o ličnosti treba da bude direktno dostavljena dotičnim pojedincima, osim ako to ne bi uključilo *nesrazmerne napore*. U tom slučaju će umesto toga biti javna komunikacija ili slična mera kojom se pojedinci obaveštavaju na jednako delotvoran način (čl. 34 st. 3 c) OUZP). Primeri transparentnih komunikacionih metoda uključuju direktne poruke (npr. e-mejla, SMS), obaveštenja putem veb stranice, poštanske komunikacije i istaknute reklame u štampanim medijima.

Uslovi u kojima *obaveštenje pojedinaca* u slučaju povreda bezbednosti podataka o ličnosti *nije potrebno* su (čl. 34 st. 3 OUZP):

- ✓ ako je rukovalac preduzeo odgovarajuće tehničke i organizacione zaštitne mere i te mere su primenjene na podatke o ličnosti u vezi sa kojima je došlo do povrede bezbednosti podataka o ličnosti, a pre svega mere koje podatke o ličnosti čine nerazumljivima licu koje nije ovlašćeno da im pristupi, kao što je enkripcija;
- ✓ ako je rukovalac preduzeo naknadne mere kojima se obezbeđuje da više nije verovatno da će doći do visokog rizika za prava i slobode lica na koja se podaci odnose; i
- ✓ ako bi to zahtevalo nesrazmeran napor. U takvom slučaju se objavljuje javno obaveštenje ili se preduzima slična mera kojom se lica na koja se podaci odnose obaveštavaju na jednako delotvoran način.

U skladu sa principom društvene odgovornosti (čl. 5 st. 2 OUZP), rukovaoci bi trebali biti u mogućnosti da demonstriraju nadležnom organu da ispunjavaju jedan ili više ovih uslova. To znači da su u stanju da dokažu da je jedan od uslova za neobaveštavanje pojedinaca ispunjen. Ako se rukovalac odluči da ne prijavi povredu bezbednosti podataka pojedincima nadzorni organ može zatražiti da to učini, ako smatra da će povreda verovatno rezultirati visokim rizikom za pojedince (čl. 34 st. 4 OUZP). [220]

12.3. Generalne obaveze rukovaoca i obrađivača

12.3.1. Procena rizika i procena visokog rizika

Kao što je već navedeno obaveza prijavljivanja tj. obaveštavanja o povredama bezbednosti podataka o ličnosti nije neophodna u svim okolnostima, već u sledećim situacijama:

- ✓ nadležni nadzorni organ potrebno je obavestiti, ako je *verovatno* da će povreda bezbednosti podataka predstavljati *rizik* za prava i slobode pojedinaca.
- ✓ obaveštenje o povredi bezbednosti podataka prema pojedincu se pokreće samo tamo gde je *verovatno da će doći do visokog rizika* za njihova prava i slobode.

Rukovalac treba odmah nakon što postane svestan povrede ne samo da spreči incident, već i da proceni rizik koji bi mogao da bude rezultat toga. Na ovaj način će rukovalac moći da sazna koja je verovatnoća i potencijalna težina uticaja na pojedinca,

[220] *Ibidem*, str. 20, 21, 22.

što mu može pomoći da preduzme efektivne korake da spreči ili reši pretnju po bezbednost podataka. Osim toga procena rizika će pomoći rukovaocu *da utvrdi da li je potrebno da obavesti nadzorni organ i pojedince*.

Procena uticaja u vezi sa zaštitom podataka (čl. 35 OUZP) razmatra rizike obrađivanja podataka kako je planirano, kao i rizike u slučaju povrede bezbednosti podataka. Ova procena predstavlja *procenu hipotetičkog događaja*. Ukoliko se stvarna povreda bezbednosti podataka dogodi, fokus procene se pomera u potpunosti na nastali ili realizovani rizik po pojedince.

Rukovalac treba da razmotri *specifične okolnosti povrede bezbednosti*, uključujući težinu potencijalnog uticaja i verovatnoću da se to dogodi, kada procenjuje rizik pojedinaca kao rezultat povrede bezbednosti podataka.

Radna grupa čl. 29 preporučuje za *procenu rizika* treba uzeti u obzir sledeće *kriterijume*:

1. Vrsta povrede bezbednosti podataka

Tip povrede bezbednosti podataka koji se dogodio može *uticati na nivo rizika* koji se predstavlja pojedincima. Npr. povreda poverljivosti kojom se medicinske informacije otkrivaju neovlašćenim strankama može imati drugačiji niz posledica za pojedinca u odnosu na to gde su pojedini zdravstveni detalji izgubljeni i više nisu dostupni.

2. Priroda, osetljivost i obim ličnih podataka

Pri proceni rizika ključan faktor je vrsta i osetljivost ličnih podataka koji su ugroženi zbog povrede podataka. Generalno *što su osetljiviji podaci, veći će rizik* od povrede prava pojedinaca. Međutim to važi i za druge podatke npr. obelodanjivanje imena i adrese osobe u običnim okolnostima verovatno neće prouzrokovati značajnu štetu, ali ako se ime i adresa roditelja usvojitelja otkrije rođenom roditelju, posledice mogu biti vrlo teške i za roditelja usvojitelja i za dete.

PRIMER
Povrede bezbednosti podataka koje uključuju podatke o zdravlju, lične dokumente ili finansijske podatke, kao što su detalji kreditne kartice, ako se zajedno koriste mogu se koristiti za krađu identiteta. Kombinacija ličnih podataka je tipično osetljivija od jednog podataka o ličnosti.

Nekada veoma *mala količina veoma osetljivih ličnih podataka može imati veliki uticaj na pojedinca*, a veliki broj detalja može otkriti veći spektar informacija o tom pojedincu. Povrede bezbednosti podataka koje utiču na velike količine ličnih podataka o velikom broju pojedinaca mogu imati uticaj na veliki broj pojedinaca.

3. Jednostavnost identifikacije pojedinaca

Važan faktor koji treba razmotriti prilikom procene rizika je verovatnoća odnosno *jednostavnost identifikacije pojedinaca* na osnovu dostupnih podataka. Naime od značaja je koliko je kriminalcu koji ima pristup kompromitovanim ličnim podacima potrebno vremena da identifikuje određene pojedinosti ili da uporedi podatke sa drugim informacijama kako bi identifikovao pojedince. U zavisnosti od slučaja, identifikacija može biti direktno dostupna iz ličnih podataka bez posebnih istraživanja

ili može biti izuzetno teško povezati lične podatke sa određenim pojedincem.

Identifikacija može biti direktno ili indirektno moguća kod povrede bezbednosti podataka, ali može zavisiti i od specifičnog konteksta kršenja i javne dostupnosti srodnih ličnih podataka. Ovo može biti relevantno za povredu poverljivosti i dostupnosti.

Lični podaci zaštićeni odgovarajućim nivoom enkripcije će biti nerazumljivi neovlašćenim licima bez ključa za dešifrovanje. Odgovarajuća primena pseudonimizacije takođe može da smanji verovatnoću identifikacije pojedinaca u slučaju povrede bezbednosti.

4. Ozbiljnost posledica po pojedinace

U zavisnosti od *prirode ličnih podataka* uključenih u povredu bezbednosti kao što je slučaj kod kompromitacije posebnih kategorija podataka, potencijalna šteta po pojedinaca može biti naročito ozbiljna. Ovo se naročito odnosi na slučajeve gde bi povrede bezbednosti mogle da dovedu do krađe identiteta ili prevare, fizičke štete, psiholoških poteškoća, poniženja ili gubitka reputacije. Ako se povreda bezbednosti povreda podataka odnosi na lične podatke o ugroženim pojedincima, oni bi mogli biti izloženi većem riziku od štete.

Na visinu rizika i procenu tj. ozbiljnost posledica utiče i to da li su podaci, koji se nalaze u rukama ljudi sa dobrim ili nepoznatim namerama ili su pak zlonamerni. To su situacije npr. *kada se lični podaci pošalju slučajno* na pogrešno odeljenje neke organizacije ili na organizaciju dobavljača sa kojom je firma sarađuje.

Rukovalac mora da čuva informacije o povredi bezbednosti podataka o ličnosti kao deo opšte dužnosti da vodi evidenciju kršenja. Treba razmotriti i *trajnost posledica po pojedince*, gde se uticaj može posmatrati kao veći ako su efekti dugoročni.

Povreda bezbednosti može uticati na lične podatke koji se tiču *dece ili drugih ugroženih osoba*, koji mogu biti izloženi većem riziku od opasnosti kao rezultat.

Priroda i uloga rukovaoca i njegove aktivnosti mogu uticati na nivo rizika pojedinaca kao rezultat povrede bezbednosti. Tako primera radi medicinska organizacija obrađuje posebne kategorije ličnih podataka, što znači da postoji veća pretnja po pojedince ukoliko dođe do povrede bezbednosti podataka o ličnosti.

Povreda bezbednosti može uticati na samo jednu ili nekoliko pojedinaca ili nekoliko hiljada. Generalno, *što je veći broj pogođenih lica, to povreda bezbednosti može imati veći uticaj na pojedince*. Povreda bezbednosti može imati ozbiljan uticaj na čak i jednog pojedinca, u zavisnosti od prirode ličnih podataka i konteksta u kojem su podaci kompromitovani. *Ključno je razmotriti verovatnoću i ozbiljnost uticaja na pogođene.*

Kada procenjuje rizik koji je verovatno rezultat povrede bezbednosti, rukovalac bi trebalo da razmotri kombinaciju težine potencijalnog uticaja na prava i slobode pojedinaca i verovatnoću nastanka ovih povreda. Tamo gde su posledice povreda bezbednosti teže, rizik je veći i slično gde je verovatnoća nastanka ovih posledica veća, rizik je takođe povećan.[221]

[219] *Ibidem*, str. 23, 24, 25.

12.3.2. Prekogranične povrede i povrede van EU

Kada postoji *prekogranična obrada ličnih podataka*, povreda bezbednosti može uticati na pojedince u više država članica. Čl. 33 st. 1 OUZP u ovim slučajevima predviđa da rukovalac *treba da obavesti nadležni nadzorni organ* (čl. 55 OUZP).

Kada se povreda odvija u kontekstu prekogranične obrade, a obaveštenje je potrebno, rukovalac će morati da obavesti nadležni nadzorni organ. Preporučuje se da se prilikom izrade *plana odgovora na bezbedonosni* propust izvrši procena od strane rukovaoca o tome *koji nadzorni organ je vodeći nadzorni organ tj. kome će izvršiti obaveštenje.* Za ustanovljavanje vodećeg nadzornog organa nije neophodna informacija, gde se nalaze oštećeni pojedinci ili gde je došlo do povrede bezbednosti, već samo obaveštenje. Vodeći nadzorni organ je jedini sagovornik za rukovaoca ili obrađivača u prekograničnoj obradi (čl. 56 st. 6 OUZP).

Kada obavesti vodeći nadzorni organ, rukovalac treba da pokaže, *da li je povreda bezbednosti podataka locirana i u drugim državama članicama*, i u kojoj verovatnoći je povreda uticala na podatke. Ako rukovalac ima bilo kakvu sumnju u pogledu identiteta vodećeg nadzornog organa onda bi trebalo da obavesti lokalni nadzorni organ gde je došlo do povrede bezbednosti podataka.

Kada se radi o rukovaocu koji nije osnovan u EU (čl. 3 st. 2 ili čl. 3 st. 3 OUZP) i dogodi se povreda bezbednosti, za njega postoji obaveza obaveštavanja prema čl. 33 i 34 OUZP. Rukovalac i obrađivač treba da odrede predstavnika u EU (čl. 27 OUZP) shodno čl. 3 st. 2 OUZP ako

- ✓ nude robu ili usluge u EU, ili
- ✓ prate ponašanje pojedinaca, koje se odvija unutar EU.

Preporučuje da se obavesti *nadzorni organ u državi članici u kojoj je osnovan predstavnik rukovaoca u EU*. Obrađivač podlaže obavezi obaveštavanja o povredi bezbednosti podataka o ličnosti prema rukovaocu (čl. 33 st. 2 OUZP).[222]

12.3.3. Obaveze obaveštavanja o povredama bezbednosti podataka o ličnosti obrađivača i zajedničih rukovaoca (čl. 33 i 34 OUZP)

Rukovalac zadržava opštu odgovornost za zaštitu ličnih podataka, ali obrađivač ima važnu ulogu kako bi omogućio rukovaocu da se pridržava svojih obaveza, a to uključuje i obaveštenja o kompromitacijama. Međutim, rukovalac treba da ima i *ugovore* sa svim obrađivačima u kojima je regulisana obaveza obaveštavanja rukovaoca u slučaju povreda bezbednosti podataka o ličnosti (čl. 28 st. 3 f) OUZP). Ugovorom ili drugim pravnim aktom treba propisati da obrađivač ''pomaže rukovaocu

[222] *Ibidem*, str. 17.

u osiguranju poštovanja obaveza prema čl. 32 do 36 OUZP uzimajući u obzir prirodu obrade i informacije koje su dostupne obrađivaču''.

Kada rukovalac koristi *obrađivača* i obrađivač postane svestan kršenja ličnih podataka koje obrađuje u ime rukovaoca, on mora da obavesti rukovaoca*''* bez nepotrebnog odlaganja*''* (čl. 33 st. 2 OUZP). Od značaja je da *obrađivač nije u obavezi da prvo proceni verovatnoću rizika* koji proizilazi iz povrede bezbednosti podataka pre obaveštavanja rukovaoca. Ova obaveza je na rukovaocu, koji mora da izvrši procenu, kada postaje svestan povrede bezbednosti. Obrađivač samo treba da utvrdi da li je došlo do kršenja, a zatim obavesti rukovaoca. *Rukovaoca treba smatrati «svesnim» kada ga je obrađivač obavestio o kršenju.* Obaveza obrađivača da obavesti svog rukovaoca omogućava rukovaocu da utvrdi da li je potrebno obavestiti nadzorni organ (čl. 33 st. 1 OUZP) i pogođena lica (čl. 34 st. 1 OUZP).

OUZP ne reguliše vremenski rok u kojem obrađivač mora da obavesti rukovaoca, osim što to mora učiniti *''*bez nepotrebnog odlaganja*''*. Stoga se preporučuje da obrađivač odmah obaveštava rukovaoca, uz dodatne informacije o povredi bezbednosti u fazama, pošto bude poznato više detalja. Ovo je od značaja kako bi se pomoglo rukovaocu da ispunjava uslove obaveštavanja nadzornom organu u roku od 72 sata.

Ugovor između rukovaoca i obrađivača treba da precizira kako treba ispuniti uslove obaveštavanja. Može biti regulisan zahtev za rano obaveštenje od strane obrađivača.

Osim toga može se regulisati, da u slučaju da obrađivač pruža usluge za više rukovaoca, koji su pogođeni istim incidentom, obrađivač treba da prijavi detalje o incidentu svakom obrađivaču.

Takođe može biti regulisano da obrađivač može da obavi obaveštenje u ime rukovaoca, ako je rukovalac dao obrađivaču odgovarajuće odobrenje. Ovakvo obaveštenje bi trebalo da bude sprovedeno u skladu sa čl. 33 i 34 OUZP. Međutim, važno je napomenuti da *zakonska odgovornost za obaveštavanje i dalje ostaje kod rukovaoca*.

Zajednički rukovaoci treba da utvrde (najbolje *ugovorom*) svoje obaveze i odgovornosti vezano za usklađenost sa OUZP (čl. 26 OUZP). Dogovor treba da utvrdi koja će strana biti odgovorna za ispunjavanje obaveza iz čl. 33 i 34 OUZP.[223]

12.3.4. Uloga ovlašćenog lica za zaštitu podataka

Kod povreda bezbednosti i obaveštenja obavezni zadaci ovlašćenog lica za zaštitu podataka uključuju *pružanje saveta i informacija o zaštiti podataka* rukovalacu ili obrađivaču. Ovlašćeno lice za zaštitu podataka takođe mora da *sarađuje sa nadzornim organom* i da deluje kao *kontakt osoba za nadzorno telo i za pojedince.*

[223] *Ibidem*, str. 11, 12, 13.

Kod obaveštavanja o povredi bezbednosti nadležnom organu rukovalac mora da pruži ime i kontakt podatke o ovlašćenom licu za zaštitu podataka ili druge kontakt osobe od koje može dobiti informacije (čl. 33 st. 3 b) OUZP).

Ovlašćeno lice za zaštitu podataka bi trebalo da odigra ključnu ulogu u prevenciji ili pripremi kod povreda bezbednosti pružanjem saveta i praćenjem usaglašenosti, kao i tokom trajanja povreda bezbednosti (obaveštavanje nadzornog organa), ali i tokom bilo kakve naknadne istrage od strane nadzornog organa. Preporučuje se da se ovlašćeno lice za zaštitu podataka odmah informiše o postojanju povreda bezbednosti i da bude uključeno u proces upravljanja povredama i obaveštenja.[224]

12.3.5. Odgovornost i vođenje evidencije (dokumentovanje povreda bezbednosti)

Bez obzira na to da li je kod povrede bezbednosti potrebno obavestiti nadzorni organ, rukovalac *mora voditi dokumentaciju o svim povredama bezbednosti* (čl. 33 st. 5 OUZP). Ova obaveza je proizlazi iz principa društvene odgovornosti (čl. 5 st. 2 OUZP). Nadzorni organ može da traži od rukovaoca spisak ili evidenciju neprijavljenih povreda bezbednosti, kao i obaveštenja o povredama bezbednosti (čl. 24 OUZP).

Rukovalac treba da evidentira *detalje o povredi bezbednosti* kao što su svi uzroci, šta se dogodilo i kako je povreda bezbednosti uticala na lične podatke. Osim toga treba uključiti efekte i posledice kršenja, zajedno sa preduzetim merama koje je rukovalac preduzeo.

OUZP ne navodi period čuvanja takve dokumentacije, pa će rukovalac ako evidencija sadrži lične podatke morati da odredi odgovarajući *period čuvanja dokumentacije* u skladu sa principima vezanim za obradu ličnih podataka. Čuvanje će bi trebalo da bude dugačko u onoj meri u kojoj je potrebno da ova dokumentacija služi kao dokaz usklađenosti sa čl. 33 st. 5 OUZP ili sa načelom odgovornosti čl. 5 st. 2 OUZP prema nadzornom organu.

Preporučuje se da rukovalac takođe dokumentuje svoje *obrazloženje za odluke* koje su preduzete kao odgovor na povredu bezbednosti. Ako ne bude obaveštenja o povredi bezbednosti, opravdanje za tu odluku treba dokumentovati i navesti razloge zbog kojih rukovalac smatra da povreda verovatno neće dovesti do rizika za prava i slobode pojedinaca. Isto tako, kada rukovalac smatra da je ispunjen bilo koji od uslova da se pojedinci ne trebaju obavestiti (čl. 34 st. 3 OUZP), onda bi trebalo da bude u mogućnosti da obezbedi odgovarajuće dokaze da je to slučaj.

Kada rukovalac odloženo obaveštava povredu bezbednosti nadležnom organu, treba da navede *razloge za to kašnjenje i da kašnjenje dokumentuje*, kako bi pokzao i dokazao opravdanost kašnjenja.

Rukovalac u komunikaciji sa pogođenim pojedincima treba da bude *transparentan o povredi bezbednosti*. On treba da demonstrira odgovornost i da dokaze takvu komunikaciju.

[224] *Ibidem*, str. 28.

U ispunjavanju OUZP (čl. 33 i 34 OUZP) rukovaoci i obrađivači bi trebalo da imaju *dokumentovan postupak obaveštavanja*. Tu se misli na proces otkrivanja povreda bezbednosti, sprečavanja povreda bezbednosti, upravljanja i reakcije na incident, kao i procene rizika i obaveštavanja o povredi bezbednosti. Pored toga, kako bi se pokazala usklađenost sa OUZP bi bilo korisno pokazati da su *zaposleni upoznati sa postojanjem takvih postupaka* i mehanizama i da znaju reagovati na povrede bezbednosti. Svakako dobar dokaz bi bila *obuka zaposlenih.*[225]

12.4. Primeri kada treba obaveštavati nadzorni organ/pojedince

Navedeni primeri potiču od Radne grupe član 29 i treba da pomognu rukovaocima u određivanju da li treba da obaveštavaju pri povredi bezbednosti ličnih podataka. Ovi primeri mogu da pomognu i u razlikovanju rizika i visokog rizika za prava i slobode pojedinaca.

Primer	*Da li treba obavestiti nadzorni organ?*	*Da li treba obavestiti pojedince?*	*Napomena/ preporuka*
Rukovalac je sačuvao sigurnosnu kopiju arhive ličnih podataka šifrovanih na USB ključu. Ključ je ukraden tokom kompromitacije.	Ne.	Ne.	Sve dok su podaci kriptovani sa najsavremenijim algoritmom, postoje rezervne kopije podataka, jedinstveni ključ nije kompromitovan, a podaci mogu biti obnovljeni u kratkom vremenu, to neće biti povreda bezbednosti koju treba prijaviti. Međutim, ako je kasnije došlo do kompromitacije, obaveštenje je potrebno.
Rukovalac pruža onlajn usluge. Kao rezultat sajber napada na te usluge, lični podaci su izfiltrirani. Rukovalac ima klijente u jednoj državi članici.	Treba izvestiti nadzorni organ ako je verovatno da će biti kompromitacije podataka pojedinaca.	Treba izvestiti pojedince, u zavisnosti od prirode ličnih podataka koji su pogođeni i ako su potencijalne posledice po pojedince sa visokim stepenom verovatnoće.	Treba izvestiti pojedince u zavisnosti od prirode pogođenih podataka o ličnosti i ako postoji visoka ozbiljnosti i verovatnoća posledica po pojedince.

[225] *Ibidem*, str. 26, 27.

Kratak prekid napajanja koji traje nekoliko minuta u centru za poziv rukovaoca što znači da klijenti nisu u mogućnosti da pozovu rukovaoca i pristupe njihovoj evidenciji.	Ne.	Ne.	Ovo nije povreda koja se treba prijaviti, ali se treba evidentirati incident shodno (čl. 33 st. 5 OUZP). Odgovarajuće dokaze treba da vodi rukovalac.
Rukovalac je pretrpeo napad ransomware koji rezultira sa šifriranim podacima. Nema rezervnih kopija i podaci se ne mogu vratiti. Tokom istrage je utvrđeno da je jedina funkcionalnost ransomwarea bila šifrovanje podataka i da u sistemu nije bilo drugih malvera.	Treba izvestiti nadzorni organ, ako postoji verovatnoća posledica po pojedince kao što je gubitak dostupnosti informacija.	Teba izvestiti pojedince, u zavisnosti od prirode ličnih podataka koji su pogođeni i potencijalnih efekata na gubitak dostupnosti podataka kao i drugih verovatnih konsekvenci.	Ukoliko postoji backup, podaci se mogu povratiti u kratkom roku, pa neće biti potrebe da se ovo prijavi nadzornom organu ili pojedincima, jer neće biti trajnog gubitka dostupnosti ili poverljivosti podataka. Ali, ako nadzorni organ sazna za incident iz drugih izvora, može se razmotriti istraga kako bi se procenila usaglašenost sa bezbednosnim zahtevima iz člana 32.
Telefonskom call centru banke prijavljena je kompromitacija podataka. Pojedinac je dobio mesečni obračun za nekog drugog. Rukovalac sprovodi kratku istragu i utvrdio je, da je došlo do kompromitacije ličnih podataka i da postoji sistemska greška koja može da znači da će i druge osobe biti ili mogu biti pogođene.	Da.	Samo pogođeni pojedinci treba da budu obavešteni, ako postoji visok rizik i potpuno je jasno da ostali nisu pogođeni.	Ako se posle dalje istrage utvrdi da je više pojedinaca pogođeno, treba ponovo poslati obaveštenje nadzornom organu i obavestiti ostale pojedince, ako postoji visok rizik.
Rukovalac upravlja onlajn šopom i ima klijente u više država. Onlajn šop je pretrpeo sajber napad. Korisnička imena, lozinke i istorija kupovine su objavljeni na mreži.	Da treba obavestiti vodeći nadzornog organa, ako se radi o prekograničnoj obradi podataka.	Da, pošto može dovesti do visokog rizika.	Rukovalac treba da preduzme akcije, npr. primoravajući promenu lozinke na pogođenim računima, kao i druge korake za ublažavanje rizika.

Firma koja se bavi hosting uslugama za veb sajtove koja deluje kao obrađivač identifikovala je grešku u kodu, koja kontroliše autentifikaciju korisnika. Efekat greške podrazumeva da svaki korisnik može pristupiti detaljima iz naloga bilo kog drugog korisnika.	Kao obrađivač (firma za hosting veb sajtova) mora da obavesti bez odlaganja pogođene klijente (rukovaoce). Ako je obrađivač sproveo sopstvenu istragu, pogođeni rukovaoci bi trebalo da budu sigurni da je svako pretrpeo povredu bezbednosti i stoga će "postati svestan" kada ih obavesti hosting kompanija (obrađivač). Rukovalac mora da obavesti nadležni organ.	Ako ne postoji verovatnoća visokog rizika, nije potrebno obavestiti pojedince.	Ako nema dokaza o tome da se ova ranjivost eksploatiše kod bilo kog od njegovih rukovaoca, možda se nije desila povreda koja treba da se prijavi, ali je potrebno dokumentovati je.
Medicinska arhiva iz bolnice nije bila dostupna 30 sati posle sajber napada.	Da, bolnica je u obavezi da obavesti pacijente ako se radi o visokom riziku.	Da, treba obavestiti pogođene pojedince.	
Podaci o ličnosti od velikog broja studenta su greškom poslati u mejl listi sa preko 1000 primaoca.	Da, treba obavestiti nadzorni organ.	Da, treba obavestiti pojedince u zavisnosti od obima i vrste podataka o ličnosti i verovatnoće nastupanja posledice.	
Kod direktnog marketinga poslat je mejl primaocu preko "to:" ili "cc:" polja i omogućeno svakom primaocu da vidi mail-adresu drugih primaoca.	Da, treba obavestiti nadzorno telo, ako se radi o velikom broju pogođenih pojedinaca, ili se radi o osetljivim podatcima (mejl lista pacijenata) ili se radi o drugim faktorima koji predstavljaju visok rizik (npr. mejl sadrži inicijalne šifre).	Da, treba obavestiti pojedince zavisno od obima i vrste podatka o ličnosti koji su uključeni i od očekivanih posledica.	Obaveštenje možda neće biti potrebno, ako se ne radi o osetljivim podacima i ako se radi o malom broju mejl adresa koje su pogođene.

13. OVLAŠĆENO LICE ZA ZAŠTITU PODATAKA „Data Protection Officer“ (čl. 37, 38 i 39 OUZP)

Stupanjem na snagu OUZP 25. maja 2018. godine uvedena je po prvi put u pravo zaštite podataka obaveza za određene rukovaoce i obrađivače da imenuju ovlašćeno lice za zaštitu podataka. Sama institucija ovlašćenog lica za zaštitu podataka je postojala i shodno Direktivi 95/46/EZ, ali organizacije nisu bile u obavezi da ga imenuju.

Rukovaocima se u velikom broju slučajeva preporučuje dobrovoljno imenovanje ovlašćenog lica za zaštitu podataka, čak i ako to OUZP izričito ne zahteva.

Organizacije koje su do sada imale ovlašćeno lice za zaštitu podataka kao glavne prednosti su isticali pouzdanost i usklađenost sa zakonom, prednost u odnosu na konkurenciju. Olakšavanje usklađivanja sa zakonom ovlašćena lica za zaštitu podataka postizali su uz instrumente za osiguranje pouzdanosti (kao što su olakšanje procene uticaja u vezi sa zaštitom podataka i spovođenje ili olakšanje revizije. Osim toga delovali su kao posrednici između zainteresovanih strana (npr. nadzornih tela, pojedinaca i poslovnih jedinica unutar organizacija).

Shodno OUZP ovlašćeno lice za zaštitu podataka ne odgovara lično za neusklađenost sa uredbom. Odgovornost za usklađenost sa OUZP snose rukovalac ili obrađivač, koji moraju da dokažu da se obrada podataka sprovodi u skladu sa uredbom (čl. 24. st. 1 OUZP).

Rukovalac ili obrađivač imaju ključnu ulogu u omogućivanju delotvorno obavljanje zadataka ovlašćenog lica za zaštitu podataka. Samo imenovanje je važno zbog usklađenosti sa OUZP, ali pored imenovanja ovlašćeno lice za zaštitu podataka treba da ima dovoljan nivo nezavisnosti i sredstava kako bi efikasno obavljao svoje zadatke.

13.1. Imenovanje ovlašćenog lica za zaštitu podataka (čl. 37 OUZP)

Obaveza imenovanja ovlašćenog lica zaštitu podataka (čl. 37 st. 1 a) OUZP) važi za sve *organe javne vlasti ili javna tela* (bez obzira na to koje podatke obrađuju).

U OUZP nije definisan pojam „organi javne vlasti ili javna tela“, a definicija ovog pojma je od značaja pošto za ove organe postoji obaveza imenovanja ovlašćenog lica zaštitu podataka. Radna grupa član 29 smatra da je taj pojam potrebno odrediti u okviru nacionalnog prava. To je iz razloga što organi javne vlasti i javna tela mogu da uključuju nacionalna, regionalna i lokalna tela, ali je moguće da ovaj pojam obuhvata i niz drugih tela koja su uređena javnim pravom. Javne poslove mogu da obavljaju i izvršavaju ne samo organi javne vlasti ili javna tela nego i druga fizička ili pravna lica, koje posluju u skladu sa javnim pravom ili privatnim pravom. Ovo se pre svega odnosi na sektore kao što su usluge javnog prevoza, snabdevanje vodom i električnom energijom, putna infrastruktura, javne radiodifuzne usluge, izgradnja socijalnih stanova itd. Radna grupa član 29 smatra kao dobru praksu za privatne organizacije koje obavljaju javne poslove ili izvršavaju javna ovlašćenja preporučuje

imenovanje ovlašćenog lica za zaštitu podataka, iako u ovom slučaju ne postoji obaveza imenovanja ovlašćenog lica zaštitu podataka.

U slučaju da se organizacija odluči da dobrovoljno imenuje ovlašćeno lice zaštitu podataka, odredbe OUZP (čl. 37-39) se primenjuju u odnosu na njegovo se imenovanje, položaj i zadatke.

Osim javnog sektora obaveza imenovanja ovlašćenog lice zaštitu podataka važi za ostale organizacije (čl. 37 st. 1 b) i c) OUZP)

- ✓ čija se osnovna delatnost sastoji u *sistematskom i masovnom praćenju pojedinaca* ili
- ✓ u *obradi posebnih kategorija podataka o ličnosti* (tzv. osetljivih podataka) u velikoj meri ili
- ✓ u *obradi podataka u velikoj meri koji se odnose na krivičnu i prekršajnu osuđivanost*.

Izuzev u slučajevima kada je očigledno da organizacija nije u obavezi da imenuje ovlašćeno lica zaštitu podataka, preporučuje se da rukovalac i obrađivač *dokumentuju sprovedene analize neophodnosti imenovanja* ovlašćenog lica zaštitu podataka. Dokumentacija o proceni i analizi služi kao dokaz da su svi relevantni činioci uzeti u obzir. Ovu analizu treba posmatrati kao deo dokumentacije prikupljene u skladu sa načelom društvene odgovornosti (čl. 5 st. 2 OUZP).

Ovlašćeno lice zaštitu podataka se imenuje za sve postupke obrade, koje obavlja rukovalac ili obrađivač. Organizacija *može da angažuje i spoljnje konsultante*, koji bi obavljali poslove ovlašćenog lica zaštitu podataka. Takođe organizacije mogu angažovati i spoljne saradnike u pogledu pomoći vezane za implementaciju OUZP, ali je u tom slučaju od značaja razgraničiti ove uloge od uloge ovlašćenog lica zaštitu podataka.[226]

Za obavezu imenovanja ovlašćenog lica zaštitu podataka potrebno je protumačiti pojam „*osnovne delatnosti*" rukovaoca ili obrađivača (čl. 37 st. 1 b) i (c) OUZP). Osnovne delatnosti rukovaoca odnose se na njegove primarne delatnosti i ne odnose se na obradu osobnih podataka kao dodatne delatnosti (U.t.r. 97 OUZP). „Osnovne delatnosti" su ključni postupci nužni za ostvarenje ciljeva rukovaoca ili obrađivača. Osnovne delatnosti uključuju *delatnosti u kojima obrada podataka čini neodvojiv deo delatnosti rukovaoca* ili *obrađivača*.

PRIMER
Osnovna delatnost bolnice je pružanje zdravstvene nege. Bolnica ne bi mogla na bezbedan način i efikasno da pruži zdravstvenu negu bez obrade zdravstvenih podataka poput zdravstvenih kartona pacijenata. Zato obradu podataka u bolnicama treba smatrati jednom od osnovnih delatnosti svake bolnice i stoga bolnice moraju imenovati ovlašćeno lice za zaštitu podataka.

[226] Radna grupa član 29, Die Datenschutzgruppe Artikel 29, *Smernice o ovlašćenom licu za zaštitu podataka*, Leitlinien in Bezug auf Datenschutzbeauftragte, usvojeno 13.12.2016., revidirano 05.o4.2017., 16/DE, WP 243 rev.01, Str. 4, 6, 7.

PRIMER
Privatno preduzeće koje se bavi bezbednošću i nadzire više privatnih trgovačkih centara i javnih prostora. Nadzor je osnovna delatnost tog preduzeća, što je nerazdvojno povezano sa obradom podataka o ličnosti. Zbog toga i ovo preduzeće mora da imenuje ovlašćeno lice za zaštitu podataka.

PRIMER
Sve organizacije obavljaju određene delatnosti, kao što je plaćanje zaposlenih ili imaju standardnu IT podršku. Ovo su pomoćne funkcije neophodne za osnovne delatnosti ili osnovno poslovanje organizacije. Iako su ove delatnosti potrebne ili ključne, obično se smatraju pomoćnim funkcijama, a ne osnovnom delatnosti.

Da bi se radilo o obaveznom imenovanju ovlašćenog lica za zaštitu podataka obrada podataka o ličnosti mora biti *u "velikom obimu"* (čl. 37 st. 1 b) i c) OUZP). Smernice za tumačenje ovog pojma su date u U.t.r. 91 OUZP, ali se one odnose na procenu uticaja u vezi sa zaštitom podataka. Preciznu definiciju količine podataka koji se obrađuju ili broja pogođenih lica nije moguće brojkom obuhvatiti, koja bi bila primenjiva u svim situacijama.[227]

Radna grupa član 29 preporučuje da se, kad se utvrđuje da li se radi o *obradi velikog obima* u obzir uzmu sledeći *kriterijumi*:

- ✓ broj pogođenih lica, odnosno njihov konkretan broj ili njihov udeo u relevantnom stanovništvu,
- ✓ količina podataka i/ili obim osetljivih podataka koji se obrađuju,
- ✓ trajanje ili trajnost aktivnosti obrade podataka,
- ✓ geografska rasprostranjenost aktivnosti obrade.

Radna grupa član 29 dala je i *primere obrada velikog obima*:

- ✓ obrada podataka o pacijentima u okviru redovnog poslovanja bolnice,
- ✓ obrada podataka o putovanjima pojedinaca koji se koriste sistem javnog gradskog prevoza (npr. praćenje uz pomoć putnih kartica),
- ✓ obrada podataka u realnom vremenu u pogledu geografske lokacije klijenata međunarodnog lanca brze hrane u statističke svrhe koju sprovodi rukovalac specijalizovan za te aktivnosti,

[227] U.t.r. 91 OUZP „obrade velikog obima čiji je cilj obrada značajnih količina podataka o ličnosti na regionalnom, nacionalnom ili nadnacionalnom nivou i koje bi mogle da utiču na veliki broj lica na koje se podaci odnose i koje će verovatno prouzrokovati veliki rizik, na primer zbog osetljivosti, kod kojih se u skladu sa dostignutim nivoom tehnološkog znanja nova tehnologija koristi u velikom obimu, kao i na druge radnje obrade koji prouzrokuju veliki rizik". U uvodnoj tački razmatranja izričito se navodi da „obradu podataka o ličnosti *ne treba smatrati obimnom* ako se odnosi na *podatke o ličnosti pacijenata ili klijenata pojedinačnih lekara, drugog zdravstvenog radnika ili advokata"*. Treba imati na umu da se ta uvodna tačka razmatranja se odnosi na procenu uticaja u vezi sa zaštitom podataka. To znači da bi određeni delovi mogli biti specifični određeni kontekst i nisu nužno na isti način primjenjivi na imenovanje ovlašćenog lica za zaštitu podataka.

- ✓ obrada podataka o klijentima u okviru redovnog poslovanja osiguravajućih društva ili banaka,
- ✓ obrada ličnih podataka od strane internet pretraživača radi bihevioralnog oglašavanja,
- ✓ obrada podataka (sadržaj, saobraćaj, lokacija podataka) koju sprovode pružaoci telefonskih ili internet usluga.

Primeri obrade koja nije velikog obima obuhvataju:

- ✓ obrada podataka pacijenta koju sprovodi samo jedan lekar,
- ✓ obrada podataka koji se odnose na krivične presude i krivična dela koju sprovodi samo jedan advokat.

Pojam *„redovno i sistematsko praćenje"* u OUZP takođe nije definisan. U U.t.r. 24. OUZP spominje pojam „*praćenje ponašanja lica*" kojim su jasno obuhvaćeni svi oblici praćenja i izrade *profila (profilisanje)* na internetu (i u svrhe bihevioralnog oglašavanja). Pojam praćenja nije ograničen samo na internet okruženje, stoga se je praćenje na internet samo jedan od primera praćenja ponašanja lica.

Radna grupa član 29 pojam „*redovno praćenje*" tumači kao:

- ✓ praćenje koje je trajno ili se sprovodi u određenim intervalima u određenom periodu,
- ✓ praćenje koje se iznova sprovodi ili ponavlja u tačno određeno vreme,
- ✓ praćenje koje se sprovodi stalno ili periodično.

Radna grupa član 29 pojam „*sistematsko praćenje*" tumači kao:

- ✓ praćenje koje se sprovodi u skladu sa određenim sistemom,
- ✓ praćenje koje je dogovoreno, organizovano ili metodično,
- ✓ praćenje koje je deo opšteg plana za prikupljanje podataka,
- ✓ praćenje koje se sprovodi kao deo strategije.

PRIMERI AKTIVNOSTI REDOVNOG I SISTEMATSKOG PRAĆENJA POJEDINACA
Upravljanje telekomunikacionom mrežom, pružanje telekomunikacionih usluga, preusmeravanje elektronske pošte, marketinške aktivnosti koje se baziraju na podacima, izrada profila i ocena radi procene rizika (npr. radi ocene kreditnog boniteta u postupku dodele kredita, određivanja premije osiguranja, mere za sprečavanje prevara, otkrivanja pranja novca), praćenje lokacije (npr. uz pomoć mobilnih aplikacija), programi vernosti, bihevioralno oglašavanje, praćenja podataka o opštem stanju organizma, telesnoj kondiciji i zdravlju uz pomoć uređaja koji se nose na telu, video nadzor, povezani uređaji (npr. pametna brojila, pametni automobili, kućna tehnika itd).

Čl. 37. st. 1 c) OUZP govori o „*posebnim kategorijama podataka i podacima o ličnosti koji se odnose na krivičnu i prekršajnu osuđivanost*“. Iako je u ovom članu upotrijebljen veznik „i”, ne postoji razlog zbog kojeg bi ova dva kriterijuma trebalo zajedno da se primenjuju. Stoga bi ovu očiglednu grešku trebalo tumačiti kao da se radi o vezniku „ili”.[228]

13.1.1. Ovlašćeno lice za zaštitu podataka od obrađivača

Pravila za imenovanje ovlašćenog lica za zaštitu podataka (čl. 37 OUZP) primjenjuju se na rukovaoce i obrađivače. U zavisnosti od toga o kojoj ulozi se radi i ko ispunjava kriterijume za obavezno imenovanje treba imenovati ovlašćeno lice za zaštitu podataka. Sama uloga *u procesu obrade podataka ne utiče na to da li će rukovalac ili obrađivač biti u obavezi da imenuje ovlašćeno lice za zaštitu podataka*. To znači da kada rukovalac ispunjava kriterijume za imenovanje, to ne znači da će to morati da uradi i njegov obrađivač.

PRIMER
Malo porodično preduzeće koje posluje u sektoru distribucije kućnih aparata u samo jednom gradu koristi usluge obrađivača čija je osnovna delatnost u pružanju usluga analize internet stranica i pomoći u ciljanom oglašavanju i marketingu. Delatnosti porodičnog preduzeća i njegovih kupaca ne iziskuju „obradu u velikom obimu” s obzirom na mali broj kupaca i relativno ograničenu delatnost. Sa druge strane aktivnosti obrađivača koji ima brojne klijente, iako bi se radilo o malom preduzeću, sveukupno zahtevaju obavljanje obrade u velikom obimu. Zbog toga obrađivač mora da imenuje ovlašćeno lice za zaštitu podataka (čl. 37 st. 1 b) OUZP). Sa druge strane porodično preduzeće nije u obavezi da imenuje ovlašćeno lice za zaštitu podataka

PRIMER
Srednje veliko preduzeće za proizvodnju pločića angažovalo je radi pružanja usluga zaštite zdravlja na radu eksternog obrađivača, koji ima veliki broj sličnih klijenata. Obrađivač mora da imenuje ovlašćeno lice za zaštitu podataka (čl. 37 st. 1 c) OUZP) pod uslovom da se radi o obradi u velikom obimu. U ovom slučaju proizvođač nije u obavezi da imenuje ovlašćeno lice za zaštitu podataka.

Ovlašćeno lice za zaštitu podataka kojeg je imenovao obrađivač dužno je da nadgleda i aktivnosti organizacije koja podatke obrađuje kad deluje samostalno kao rukovalac (npr. obrada podataka zaposlenih, logistika itd.).

[228] *Ibidem*, str. 8, 9, 10.

13.1.2. Imenovanje jednog ovlašćenog lica za zaštitu podataka za više organizacija

Grupacija povezanih društava (čl. 37 st. 2 OUZP) može da imenuje jedno ovlašćeno lice za zaštitu podataka pod uslovom da je „lako dostupan iz svake poslovne jedinice". *Pojam dostupnosti* odnosi se na dostupnost prema pojedincima (čl. 38 st. 4 OUZP), prema nadzornom organu (čl. 39. st. 1 e) OUZP), ali i u okviru organizacije „informisanje i savetovanje rukovaoca ili obrađivača i zaposlenih koji vrše obradu o njihovim obavezama u skladu s ovom uredbom". Da bi se obezbedila dostupnost ovlašćenog lica za zaštitu podataka potrebno je da su njegovi podaci za kontakt dostupni u skladu sa OUZP.

Sama dostupnost treba da bude delotvorna, te stoga Radna grupa član 29 preporučuje da *ovlašćeno lice za zaštitu podataka bude smešteno na teritoriji EU* bez obzira na to da li rukovalac ili obrađivač ima poslovno predstavništvo u EU.

Ovlašćeno lice za zaštitu podataka mora da bude u mogućnosti da delotvorno *komunicira* sa *pojedincima* (čl. 12 st. 1 OUZP) i *sarađuje sa nadzornim organom* (čl. 39 st. 1 d) OUZP). Komunikacija se mora odvijati na jeziku ili jezicima koje upotrebljava nadzorni organ i pojedinci.

Ako se radi o *rukovaocu ili obrađivaču koji je telo javne vlasti ili javno telo*, može se *imenovati jedno ovlašćeno lice za zaštitu podataka* (čl. 37 st. 3 OUZP).

13.1.3. Stručno znanje i veštine ovlašćenog lica za zaštitu podataka

U pogledu kvalifikacija regulisano je sledeće (čl. 37 st. 5 OUZP): „ovlašćeno lice za zaštitu podataka imenuje se na osnovu *stručnih kvalifikacija*, a posebno *stručnog znanja o zakonodavstvu i praksi u oblasti zaštite podataka i sposobnosti* obavljanja zadataka iz člana 39.". Neophodan nivo stručnog znanja bi trebalo utvrditi *u odnosu na postupke obrade podataka koji se sprovode i u odnosu na obaveznu zaštitu podataka o ličnosti* koji se obrađuju (U.t.r. 97 OUZP).

Obavezan nivo stručnosti nije definisan, ali on mora biti srazmeran osetljivosti, složenosti i količini podataka koju organizacija obrađuje. Npr. ako je postupak obrade podataka naročito složen ili ako obuhvata *veliku količinu osetljivih podataka*, ovlašćeno lice za zaštitu podataka trebalo bi da ima viši stupanj stručnosti. Razlika postoji i u zavisnosti od toga da li organizacija sistematski *prenosi podatke van EU* ili su ti prenosi povremeni. Prilikom odabira ovlašćenog lica za zaštitu podataka potrebno je uzeti u obzir probleme povezane sa zaštitom podataka koji se javljaju unutar organizacije. Iako OUZP ne navodi potrebne stručne kvalifikacije, trebalo razmotriti prilikom imenovanja ovlašćenog lica za zaštitu podataka *znanje iz nacionalnog i evropskog prava i prakse*, kao i *detaljno razumevanje OUZP*.[229]

[229] Po sličnosti mogu se uzeti u obzir i zahtevi u pogledu kvalifikacija od dizeldorfskog kruga, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 24./25. November 2010), Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG), str. 1.

Korisno je i *poznavanje poslovnog sektora i organizacije rukovaoca*. Ovlašćeno lice za zaštitu podataka mora dobro da razume i *postupke obrade podataka, informacione sisteme* i potrebe rukovaoca u pogledu *bezbednosti i zaštite podataka*. Ako se radi o telu javne vlasti ili javnom telu, ovlašćeno lice za zaštitu podataka bi trebalo dobro da poznaje *upravno pravo i postupke tih organizacija*.

Sposobnost izvršavanja zadataka poverenih ovlašćenom licu za zaštitu podataka treba tumačiti u odnosu na njihove lične kvalitete i znanja u odnosu na njihov položaj u organizaciji. Npr. u lične kvalitete treba da uključi poštenje i visoku profesionalnu etiku. Ovlašćeno lice za zaštitu podataka treba prvenstveno da obezbedi poštovanje OUZP. On ima ključnu ulogu u negovanju kulture zaštite podataka unutar organizacije i pomaže u sprovođenju bitnih elemenata OUZP (načela obrade podataka, prava pojedinaca, ugrađena i podrazumevana zaštita podataka, evidencija aktivnosti obrade, bezbednost obrade kao i obaveštavanje o povredama bezbednosti podataka o ličnosti...).

13.1.4. Angažovanje, objavljivanje i saopštavanje podataka ovlašćenog lica za zaštitu podataka

U praksi je moguće zaposliti ovlašćeno lice za zaštitu podataka interno u organizaciji shodno ugovoru o radu.

Funkcija ovlašćenog lica za zaštitu podataka može se obavljati i na osnovu *ugovora o delu sklopljenog sa pojedincem ili organizacijom izvan organizacije rukovaoca ili obrađivača*. U svakom slučaju je važno *izbegavati sukob interesa*. Takođe je važno da svaki član bude zaštićen odredbama OUZP (npr. da ne bude neosnovanog raskidanja ugovora za poslove ovlašćenog lica za zaštitu podataka, ali ni neosnovaog otpuštanja lica koje obavlja zadatke ovlašćenog lica za zaštitu podataka). Zbog pravne sigurnosti i dobre organizacije preporučuje jasna raspodela poslova sa eksternim ovlašćenim licem za zaštitu podataka, kao i imenovanje kontakt osobe odgovorne za odnose sa ovlašćenim licem za zaštitu podataka. Ovo bi trebalo biti regulisano u ugovoru o delu.

Podaci ovlašćenog lica za zaštitu podataka *moraju biti objavljeni i saopšteni nadzornom organu* (čl. 37 st. 7 OUZP) od strane rukovaoca ili obrađivača. Ovim zahtevima se želi omogućiti pojedincima (unutar i izvan organizacije) i nadzornim organima jednostavno i direktno stupanje u kontakt sa ovlašćenim licem za zaštitu podataka, a da pritom ne moraju da stupe u kontakt ostalim delovima organizacije. Osim toga ovom prilikom od značaja je poverljivost: npr. da zaposleni mogu oklevati u pogledu podnošenja žalbi ovlašćenom licu za zaštitu podataka ako nije zagarantovana poverljivost njihove komunikacije. Ovlašćeno lice za zaštitu podataka je u obavezi da svoje zadatke obavlja u skladu sa profesionalnom tajnom ili poverljivošću (čl. 38 st. 5 OUZP).

Kontakt podaci ovlašćenog lica za zaštitu podataka treba da sadrže informacije koje će pojedincima i nadzornim organima omogućiti da lako dođu do ovlašćenog lica za zaštitu podataka (poštanska adresa, određeni telefonski broj i/ili određena

adresa elektroničke pošte). Ako je primenljivo za potrebe komuniciranja mogu se koristiti i druga komunikaciona sredstva npr. call centar ili obrazac za kontakt koji se upućuje ovlašćenom licu za zaštitu podataka na internet stranici organizacije.

Ime ovlašćenog lica za zaštitu podataka ne mora se navesti u obavljenim kontakt podacima (čl. 37 st. 7 OUZP). Međutim u smislu dobre prakse preporučuje se navođenje ovih podataka. *Ime ovlašćenog lica za zaštitu podataka potrebno je dostaviti nadzornom organu* kako bi ova fukncija mogla da posluži kao kontakt osoba između organizacije i nadzornog organa (čl. 39. st. 1. e) OUZP). Radna grupa član 29 smatra dobrom praksom i preporučuje da organizacija svoje zaposlene obavesti o imenu i kontakt podacima ovlašćenog lica za zaštitu podataka.[230]

13.2. Položaj ovlašćenog lica za zaštitu podataka (čl. 38 OUZP)

Učestvovanje ovlašćenog lica za zaštitu podataka u svim pitanjima koja se odnose na zaštitu podataka o ličnosti, predstavlja jednu od značajnih obaveza za rukovaoca i obrađivača. Oni trebaju da obezbede ovlašćenom licu zaštitu podataka „na odgovarajući način i blagovremeno *uključen u sva pitanja u pogledu zaštite podataka o ličnosti*" (čl. 38 st. 1 OUZP).

Od značaja je da ovlašćeno lice za zaštitu podataka bude što ranije uključeno u sva pitanja koja se odnose na zaštitu podataka.

Pri sprovođenju procene uticaja u vezi sa zaštitom podataka, rukovalac treba da uključi u najranijoj fazi ovlašćeno lice zaštitu podataka i zatraži njegovo mišljenje odnosno savet (čl. 35 st. 2 OUZP). Uključivanje ovlašćenog lica zaštitu podataka u sva pitanja zaštite podataka omogućava ne samo usklađenost sa OUZP nego i utiče na ostvarivanje pristupa integrisane zaštite privatnosti kao na deo upravljanja organizacijom. Osim toga od značaja je da ovlašćeno lice za zaštitu podataka bude uključeno i u relevantna radna tela unutar organizacije, koja se bave pitanjima obrade podataka (npr. komisije, radne grupe, komiteti itd.).

Od organizacije se zahteva podrška ovlašćenom licu zaštitu podataka u vidu *pružanja potrebnih sredstva* za izvršavanje njegovih zadataka i *ostvarivanje pristupa podacima* o ličnosti i postupcima obrade kao i za *održavanje njegovog stručnog znanja*" (čl. 38 st. 2 OUZP).

Ovi zahtevi se prema mišljenju Radne grupe član 29 ostvaruju na sledeći način:

- ✓ putem aktivne podrške rukovodstva organizacije (top menadžmenta, generalnog direktora, upravnog odbora) funkciji ovlašćenog lica za zaštitu podataka,
- ✓ kroz obezbeđivanje dovoljno vremena za ispunjavanje zadataka ovlašćenog

[230] Radna grupa član 29, Die Datenschutzgruppe Artikel 29, *Smernice o ovlašćenom licu za zaštitu podataka*, Leitlinien in Bezug auf Datenschutzbeauftragte, usvojeno 13.12.2016., revidirano 5. 04.2017., 16/DE, WP 243 rev.01, str. 11, 12, 13, 14, 15.

lica za zaštitu podataka. Naročito u slučajevima ako je ovlašćeno lice za zaštitu podataka angazovano kao spoljni saradnik po ugovoru o delu ili ako je angazovano interno, ali ne radi puno radno vreme. Dobra je praksa da se utvrdi postotak vremena predviđen za obavljanje dužnosti ovlašćenog lica za zaštitu podataka ako se ona ne obavlja u punom radnom vremenu. U ovim slučajevima je od značaja utvrditi zadatke po prioritetu i izraditi plan rada ovlašćenog lica za zaštitu podataka,

- ✓ putem obezbeđivanja odgovarajućih financijskih sredstava, infrastrukture (radni prostor, oprema itd.) i po potrebi osoblja,
- ✓ putem obaveštavanja zaposlenih o imenovanju ovlašćenog lica za zaštitu podataka kako bi se obezbedilo da su u organizaciji svi upoznati sa njegovim postojanjem i dužnostima,
- ✓ putem omogućavanja pristupa organizaciji i procesima u organizaciji, kao što su ljudski resursi, pravni zahtevi, informacione tehnologije, bezbednost itd. u svrhu podrške, saradnje i razmene informacija sa ovlašćenim licem za zaštitu podataka,
- ✓ putem omogućavanja kontinuiranog osposobljavanja, što omogućava ovlašćenom licu za zaštitu podataka da se konstantno usavršava u oblasti zaštite podataka (npr. u vidu učestvovanja na seminarima, radionicama, obukama, treninzima itd.),
- ✓ s obzirom na veličinu i strukturu organizacije može se uspostaviti tim ovlašćenog lica za zaštitu podataka (sastojao bi se od ovlašćenog lica za zaštitu podataka i njegovih saradnika). Tada je potrebno ustanoviti plan funkcionisanja tima i ponaosob zadatke i odgovornost svakog člana tima. Po sličnom modelu treba odrediti zadatke i odgovornost svakog člana tima, ako se radi o eksternom ovlašćenom licu za zaštitu podataka koji deluje organizovano kao tim.

U načelu, sto su složeniji i/ili osetljiviji postupci obrade to za ovlašćeno lice za zaštitu podataka treba izdvojiti više sredstava.

Ovlašćena lica za zaštitu podataka moraju da budu u stanju da zadatke obavljaju sa dovoljnim stepenom autonomije (čl. 38 st. 3 OUZP). Rukovalac ili obrađivač moraju da obezbede da ovlašćeno lice za zaštitu podataka „ne prima nikakve *nikakve instrukcije* prilikom obavljanja svojih zadataka". Ovlašćena lica za zaštitu podataka "bez obzira na to da li su zaposlena kod rukovaoca podataka, moraju da budu u mogućnosti da *nezavisno obavljaju* svoje dužnosti i zadatke" (U.t.r. 97 OUZP). Ovi zahtevi se odnose na nezavisno obavljanje zadataka (čl. 39 OUZP) bez davanja instrukcija npr. o načinu ispitivanja procesa, o upućivanju na drugačije tumačenje zakona, o tome da li treba tražiti savet nadzornog organa itd.

Od izuzetnog značaja je napomenuti da *rukovalac ili obrađivač i pored angažovanja ovlašćenog lica* za zaštitu podataka *ostaju odgovorni za usklađenost sa OUZP*. Ako rukovalac ili obrađivač donesu odluke nespojive sa OUZP i savetom ovlašćenog lica za zaštitu podataka, ovlašćenom licu za zaštitu podataka trebalo bi

da bude omogućeno da svoje suprotno mišljenje najvišem rukovodstvu organizacije. Ovlašćeno lice za zaštitu podataka „*odgovara neposredno najvišem nivou rukovodstva* rukovaoca ili obrađivača" (čl. 38 st. 3 OUZP). Na taj način se osigurava da najviše rukovodstvo organizacije bude upoznato sa savetima i preporukama ovlašćenog lica za zaštitu podataka. Primer dobre prakse u tom pogledu bi bio godišnji izveštaj o radu i aktivnostima ovlašćenog lica za zaštitu podataka koje se dostavlja najvišem rukovodstvu u organizaciji.

Autonomija i zaštita u obavljanju zadataka ovlašćenog lica za zaštitu podataka zagarantovane su i time što je regulisano da rukovalac ili obrađivač „*ne smeju ovlašćeno lice za zaštitu podataka da razreše dužnosti ili kazne zbog izvršavanja njegovih zadataka*" (čl. 38 st. 3 OUZP). Zabranjeno je kažnjavanje ako su kazne uvedene kao posledice toga, što je ovlašćeno lice za zaštitu podataka obavljalo svoje zadatke.

PRIMER
Ovlašćeno lice za zaštitu podataka može smatra da određena obrada verovatno izazva visok stepen rizika i savetuje rukovaocu ili obrađivaču da sprovedu procenu uticaja u vezi sa zaštitom podataka. Međutim, rukovalac ili obrađivač se ne slažu sa tom procenom i savetom ovlašćenog lica za zaštitu podataka. Ovlašćeno lice za zaštitu podataka ne može biti razrešeno dužnosti u ovoj situaciji samo zato što je na ovaj način savetovalo rukovodstvo.

Kazne mogu biti direktne ili indirektne kao npr. izostanak podrške, onemogućavanja napredovanja u karijeri, uskraćivanja pogodnosti koje dobijaju ostali zaposleni. Same kazne ne moraju da budu sprovedene, dovoljna je pretnja kaznom ako se ovlašćeno lice za zaštitu podataka kažnjava u pogledu njegovih aktivnosti i u ulozi ovlašćenog lica za zaštitu podataka. Ovo svakako ne znači da ovlašćeno lice za zaštitu podataka ni u jednom slučaju ne može biti razrešeno dužnosti. U praksi se pokazalo da je to moguće iz razloga koji nisu povezani sa izvršavanjem njegovih zadataka (npr. u slučaju krađe, fizičkog, psihičkog ili seksualnog uznemiravanja ili slične grube povrede dužnosti). Važno je istaći da *OUZP ne propisuje* kako i kada se ovlašćeno lice za zaštitu podataka može *razrešiti dužnosti* ili *zameniti*.

Ovlašćeno lice za zaštitu podataka „*može da obavlja i druge zadatke i dužnosti*", međutim organizacija mora da obezbedi da „*ti zadaci i dužnosti ne dovedu do sukoba interesa*" (čl. 38 st. 6 OUZP). Sukob interesa je povezan sa zahtevom delovanja ovlašćenog lica za zaštitu podataka na nezavisan način. Generalno je ovlašćenim lica za zaštitu podataka dopušteno da obavljaju druge dužnosti, ali obavljanje tih dužnosti i zadataka ne sme da dovode do sukoba interesa. To podrazumeva da ovlašćeno lice za zaštitu podataka ne može imati *poziciju u organizaciji koja sa sobom nosi da on odlučuje o svrsi, sredstvima i načinu obrade podataka o ličnosti*. Radna mesta koja mogu biti u sukobu interesa u okviru organizacije se odnose pre svega na položaj u višem rukovodstvu (predsednik uprave, direktor poslovanja, direktor finansija, šef marketing odeljenja, šef ljudskih resursa ili šef IT odeljenja). Sukob interesa može nastati, ako

se od eksternog ovlašćenog lica za zaštitu podataka zatraži da pred sudovima zastupa rukovaoca ili obrađivačima u slučajevima koji uključuju pitanja zaštite podataka.

Preporučuje se kao primer dobre prakse, zavisno od delatnosti, veličine i strukture organizacije da:

- ✓ utvrde funkcije koje su nespojive sa funkcijom ovlašćenog lica za zaštitu podataka,
- ✓ usvoje interna pravila kako bi se izbegao sukob interesa,
- ✓ objasni sukob interesa uopšteno,
- ✓ izjave da njihovo ovlašćeno lice za zaštitu podataka nije u sukobu interesa u odnosu na njegovu dužnost, što će doprineti podizanju svesti o postojanju te obaveze,
- ✓ se u interna pravila organizacije uvrste zaštitne mere i obezbedi da opis radnog mesta ovlašćenog lica za zaštitu podataka ili ugovor o delu bude precizano i jasno formulisan radi izbegavanja sukoba interesa. [231]

13.3. Zadaci ovlašćenog lica za zaštitu podataka (čl. 39 OUZP)

Praćenje usklađenosti sa OUZP jedan je od osnovnih zadataka ovlašćenog lica za zaštitu podataka (čl. 39 st. 1 b) OUZP). Preciziranje ove obaveze moguće je naći u U.t.r. 97 OUZP, kojom je objašnjeno da bi ovlašćeno lice za zaštitu podataka trebalo da „pomaže rukovaocu ili obrađivaču u praćenju unutrašnje usklađenosti sa ovom uredbom".

U okviru dužnosti praćenja poštovanja OUZP ovlašćeno lice za zaštitu podataka može:

- ✓ da prikuplja informacije radi utvrđivanja aktivnosti obrade,
- ✓ analizira i proverava usklađenost aktivnosti obrade i
- ✓ obaveštava rukovaoca ili obrađivača i pruža savete i preporuke.

Ovlašćeno lice za zaštitu podataka i pored toga što ima obavezu da prati usklađenost ne znači da je lično odgovorno u slučaju neusklađenosti. OUZP jasno određuje u tom pogledu odgovornost rukovaoca, koji je dužan da „sprovodi odgovarajuće tehničke i organizacione mere kako bi obezbedio da se obrada vrši u skladu s ovom uredbom kako bi to mogao da dokaže" (čl. 24 st. 1 OUZP). Samim tim je jasno da je usklađenost sa pravom zaštite podataka korporativna odgovornost rukovaoca, a ne ovlašćenog lica za zaštitu podataka.

Rukovalac, a ne ovlašćeno lica za zaštitu podataka *je dužan da sprovede procenu uticaja u vezi sa zaštitom podataka*, ako su za to ispunjeni uslovi (čl. 35 st. 1 OUZP). U ovom postupku ovlašćeno lice za zaštitu podataka ima važnu i korisnu ulogu u pružanju pomoći rukovocu. Uzimajući u obzir načelo integrisane zaštite podataka

[231] *Ibidem*, str. 16, 17, 18, 19.

izričito se zahteva da *rukovalac traži savet od ovlašćenog lica za zaštitu podataka* pri sprovođenju procene uticaja u vezi sa zaštitom podataka (čl. 35 st. 2 OUZP). Takođe OUZP sa druge strane obavezuje ovlašćeno lice za zaštitu podataka na pružanje saveta, kada je to zatraženo, u pogledu procene uticaja u vezi sa zaštitom podataka i praćenje njenog izvršavanja u skladu sa članom 35 (čl. 39 st. 1 c) OUZP).

Radna grupa član 29 preporučuje da *rukovalac potraži savet od ovlašćenog lica za zaštitu podataka po sledećim pitanjima*:

- ✓ da li treba sprovesti ili ne procenu uticaja u vezi sa zaštitom podataka,
- ✓ koju metodologiju treba primeniti pri sprovođenju procene uticaja u vezi sa zaštitom podataka,
- ✓ da li procenu uticaja u vezi sa zaštitom podataka treba sprovesti interno ili je poveriti eksternim ovlašćenim licima za zaštitu podataka,
- ✓ koje zaštitne mere (uključujući tehničke i organizacione mere) treba primeniti radi ublažavanja mogućih rizika za prava i interese pojedinaca,
- ✓ da li je procena uticaja u vezi sa zaštitom podataka pravilno sprovedena ili nije, kao i da li su zaključci (da li treba sprovesti obradu ili ne i koje su zaštitne mere primenjive) u skladu sa OUZP.

U slučaju da rukovalac nije saglasan sa savetom ovlašćenog lica za zaštitu podataka potrebno je da u *dokumentaciji o proceni uticaja u vezi sa zaštitom podataka u pisanom obliku obrazloži zašto savet nije uzet u obzir* (čl. 24 st. 1 OUZP).

Preporučuje se da rukovalac u ugovoru sa ovlašćenim licem za zaštitu podataka i u informacijama koje se dostavljaju zaposlenima, rukovodstvu jasno navede zadatke i odgovornost ovlašćenog lica za zaštitu podataka, a naročito u pogledu sprovođenja procene uticaja u vezi sa zaštitom podataka. U bitne zadatake ovlašćenog lica za zaštitu podataka spadaju „*saradnja sa nadzornim organom*" i „*delovanje kao kontaktna tačka za nadzorni organ* o pitanjima koja se tiču obrade, što uključuje i prethodne konsultacije iz člana 36, a u odgovarajućim slučajevima i savetovanje o drugim pitanjima" (čl. 39 st. 1 d) i e) OUZP). Ovi zadaci sa jedne strane olakšavaju obavljanje dužnosti ovlašćenog lica za zaštitu podataka, dok sa druge strane navođenje ovlašćenog lica za zaštitu podataka kao kontaktne tačke olakšava pristup dokumentima i informacijama nadzornom organu u obavljanju zadataka (čl. 57 i 58 OUZP).

Kao što je već istaknuto ovlašćeno lice za zaštitu podataka je u obavezi da obavlja svoje zadatke i dužnosti u skladu sa *čuvanjem profesionalne tajne ili poverljivošću* (čl. 38 st. 5 OUZP). Obaveza čuvanja tajne odnosno povjerljivost ne znači da je ovlašćenom licu za zaštitu podataka zabranjeno da se obratiti nadzornom organu i od njega zatražiti savet. Štaviše, ovlašćeno lice za zaštitu podataka *može da se posavetuje sa nadzornim organom o svim ostalim pitanjima* (čl. 39 st. 1 e) OUZP).

Ovlašćeno lice za zaštitu podataka je u obavezi da „vodi računa o *rizicima vezanim za radnje obrade* i uzima u obzir prirodu, obim, okolnosti i svrhe obrade" (čl.

39 st. 2 OUZP). Od ovlašćenog lica za zaštitu podataka se zahteva da utvrdi prioritetne aktivnosti i pažnju usmere na pitanja koja predstavljaju veći rizik u kontekstu zaštite podataka. To naravno ne znači da treba zanemariti praćenje usklađenosti postupaka obrade podataka koji nose sa sobom nizi nivo rizika, ali u fokusu bi trebalo da budu područja višeg rizika.

Ovlašćeno lice za zaštitu podataka bi shodno pristupu baziranom na riziku trebalo da pruži savete rukovaocima koju metodologiju treba da upotrebe za sprovođenje procene uticaja u vezi sa zaštitom podataka, koja područja bi trebalo podvrgnuti unutrašnjoj a koja eksternoj kontroli zaštite podataka, koje interne mere obuke treba obezbediti za zaposlene ili rukovodioce i kojim aktivnostima obrade treba posvetiti više vremena i sredstava.

Obaveza vođenja evidencija se odnosi na rukovaoce ili obrađivače, a ne na ovlašćeno lice za zaštitu podataka (čl. 30 st. 1 i 2 OUZP). U praksi ovlašćeno lice za zaštitu podataka sastavlja i vodi evidenciju postupaka obrade, ali treba imati u vidu da odgovornost i ova dužnost pogađa direktno organizaciju.

Osim toga od značaja je da čl. 39 st. 1 OUZP navodi popis zadataka ovlašćenog lica za zaštitu podataka, koji se smatra *minimalnim opisom posla ovlašćenog lica za zaštitu podataka*. Rukovalac ili obrađivač mogu stoga da dodele ulogu vođenja evidencije aktivnosti obrade podataka. Pogotovu imajući u vidu da je vođenje evidencije instrument uz pomoć koga se ovlašćenom licu za zaštitu podataka omogućava obavljanje njegovih zadataka u pogledu praćenja usklađenosti, obaveštavanja i savetovanja rukovaoca ili obrađivača.

Treba napomenuti, ma kako da je organizovano vođenje evidencije, sama evidencija mora da bude dostupna na zahtev nadzornom organu radi uvoda u sve aktivnosti obrade podataka o ličnosti. Zbog toga je evidencija preduslov za usklađenost sa OUZP i mera za obezbeđivanje saglasnosti sa načelom društvene odgovornosti. Može se reći da je sama evidencija predstavlja *ID za organizacije* u pogledu zaštite podataka! [232]

[232] *Ibidem*, str. 19, 20, 21, 22.

14. Prenos podataka (čl. 44, 45, 46 i 49 OUZP)

Većina organizacija obavlja svakakodnevno prenos podataka. On može biti u okviru EU, a takođe može biti i van EU.

PRIMERI
Firma u okviru koncerna prenosi podatke klijenata iz Španije u Poljsku svojoj firmi ćerki. Advokatska kancelarija iz Kine prima podatke iz EU od preduzeća iz različitih zemalja radi kupovine nekretnina. Računarski centar od firme iz Francuske se nalazi u Indiji.

Transfer odnosno *prenos podataka unutar EU* je generalno slobodan. *Preduslov uopšte za dopuštenost prenosa* je ispunjenje načela zaštite podataka (čl. 5 OUZP) i zakonitosti obrade (čl. 6 ili čl. 9 OUZP).

Sa druge strane *prenos podataka u „treće zemlje"* je *dopušten samo ukoliko rukovalac i obrađivač postupaju u skladu sa uslovima iz poglavlja V OUZP* (čl. 44 OUZP).

Poglavlje V OUZP se primenjuje i u slučaju „*daljih prenosa*" podataka o ličnosti iz treće zemlje ili međunarodne organizacije u drugu treću zemlju ili međunarodnu organizaciju (čl. 44 OUZP).

U praksi to dovodi do primene u sledećim situacijama:

- ✓ Rukovalac prenosi podatke korisniku u „trećoj zemlji", a treći prenosi podatke nekom daljem korisniku u „trećoj zemlji";

PRIMER
Koncern firma ćerka iz Bugarske otkriva podatke (učestvovanje u zajedničkim programima radi isplate bonusa zaposlenima u okviru koncerna) korisniku firmi ćerki u Rusiji, a firma ćerka iz Rusije otkriva podake korisniku firmi majci u Kini.

- ✓ Rukovalac prenosi podatke obrađivaču u „trećoj zemlji", a obrađivač prenosi podatke nekom daljem obrađivaču u „trećoj zemlji";

PRIMER
Klaud firma iz Poljske prenosi podatke u Tursku gde se nalaze drugi serveri, firma iz Turske prenosi dalje podatke klaud firmi u Indiji gde se takođe podaci nalaze na serverima u „oblacima".

- ✓ Rukovalac sa sedištem u „trećoj zemlji" prenosi podatke obrađivaču u EU, a obrađivač prenosi podatke daljem obrađivaču u „trećoj zemlji".

PRIMER
Klaud firma iz Srbije prenosi podatke u Mađarsku gde se nalaze drugi serveri, firma iz Mađarske prenosi dalje podatke klaud firmi u Indiji gde se takođe podaci nalaze na serverima u „oblacima".

Treba primeniti da *za prenos u treće zemlje može postojati rizik* po sebi, te *se stoga preporučuje* sprovođenje *procene uticaja u vezi sa zaštitom podataka* (čl. 35 OUZP).

U pogledu dopuštenosti prenosa podataka postoje sledeće mogućnosti:

1. Prenos se sprovodi *na osnovu odluke adekvatnosti* (čl. 45 st. 1 OUZP);
2. Prenos se sprovodi *na osnovu adekvatnih zaštitnih mera* i pod uslovom da su licima na koja se podaci odnose na raspolaganju *izvršiva prava i delotvorna pravna sredstva* (čl. 46 st. 1 OUZP);
3. Prenos podataka shodno čl. 49 OUZP *bez odluke o adekvatnosti* (čl. 45 st. 3 OUZP) *ili odgovarajućih zaštitnih mera* (čl. 46 OUZP) *uključujući i obavezujuća korporativna pravila* (čl. 47 OUZP);
4. *Poseban pravni osnov prenosa podataka* (čl. 49 OUZP poslednji pasus).

Rukovaoci ili obrađivači treba najpre da procene mogućnosti za prenos po osnovu članova 45, 46, 47 OUZP, i da mogućnost iz člana 49 OUZP iskoriste, tek onda kada to nije moguće navedenim pravnim osnovima.[233]

1. Prenos u treće zemlje sa adekvatnim nivoom zaštite podataka (čl. 45 OUZP)

Evropska komisija je još za vreme važenja Direktive iz 95. godine proglasila određeni broj trećih zemalja koje imaju *adekvatan nivo zaštite podataka, te za ove zemlje i dalje važi odluka o adekvatnom nivou zaštite podataka i po stupanju OUZP na snagu* (čl. 45 st. 9 OUZP). Shodno čl. 45 OUZP je Evropska komisija nastavila sa tom praksom. Takođe broj zemalja koji su na ovoj listi je u konstantnom porastu. [234]

Po osnovu odluke Evropske komisije, kada se treća država proglasi za zemlju sa „adekvatnim nivoom zaštite podataka“, *prenos podataka je u tu zemlju slobodan* (čl. 45 st. 1 OUZP). To znači da treća zemlja koja je na ovoj listi ima izjednačen *status u smislu prava zaštite podataka kao bilo koja država EU*.

Treće zemlje koje se nalaze na listi sa adekvatnim nivoom zaštite podataka su:

- ✓ Andora,
- ✓ Argentina,
- ✓ Kanada,
- ✓ Farska ostrva,
- ✓ Guernsej,
- ✓ Izrael,
- ✓ Ostrvo Man,
- ✓ Ostrvo Džersi,

[233] European Data Protection Board, *Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679*, angenommen am 25. Mai 2018, str. 4.

[234] Rainer Knyirm, Datenschutz-Grundverordnung, Knyrim, 2016., str. 253, 254, 255.

- ✓ Novi Zeland,
- ✓ Švajcarska,
- ✓ Urugvaj,
- ✓ Sjedinjene Američke Države.

Trenutno se vode pregovori sa Japanom i Južnom Korejom. Odluka o priznavanju adekvatnosti zaštite podataka sa Japanom je već u proceduri, te se stoga može očekivati njeno usvajanje do početka 2019. godine.[235]

Prilikom ispitivanja adekvatnosti treće zemlje kao zemlje sa odgovarajućim nivoom zaštite podataka Evropska Komisija uzima u obzir sledeće kriterijume (čl. 45 st. 2 OUZP):

- ✓ vladavinu prava, poštovanje ljudskih prava i osnovnih sloboda, relevantno opšte i sektorsko zakonodavstvo, što uključuje zakonodavstvo o javnoj bezbednosti, odbrani, nacionalnoj bezbednosti, krivičnom pravu i pristupu organa javne vlasti podacima o ličnosti, kao i primenu tog zakonodavstva, pravila o zaštiti podataka, pravila struke i mere bezbednosti, što uključuje pravila za dalji prenos podataka o ličnosti u drugu treću zemlju ili međunarodnu organizaciju, koja se poštuju u toj trećoj zemlji ili međunarodnoj organizaciji, sudsku praksu, kao i postojanje efektivnih i izvršivih prava lica na koja se podaci odnose i efikasne upravne i sudske zaštite lica čiji se podaci o ličnosti prenose;
- ✓ postojanje i delotvorno funkcionisanje jednog ili više nezavisnih nadzornih organa u trećoj zemlji ili nezavisnih nadzornih organa koji su nadležni za međunarodnu organizaciju s odgovornošću za obezbeđivanje i sprovođenje poštovanja pravila o zaštiti podataka, što uključuje adekvatna izvršna ovlašćenja za pružanje pomoći licima na koja se podaci odnose i savetovanje lica na koja se podaci odnose u ostvarivanju njihovih prava, kao i za saradnju s nadzornim organima država članica;
- ✓ međunarodne obaveze koje je dotična treća zemlja ili međunarodna organizacija preuzela ili druge obaveze koje proizilaze iz pravno obavezujućih konvencija ili instrumenata, kao i iz njenog učestvovanja u multilateralnim ili regionalnim sistemima, posebno u vezi sa zaštitom podataka o ličnosti.

Komisija *nakon procene adekvatnosti* nivoa zaštite može *aktom za sprovođenje* da odluči da se adekvatnost nivoa zaštite podataka *ispituje svake 4 godine* (čl. 45 st. 3 OUZP).

Komisija je u obavezi takođe da *kontinuirano prati razvoj događaja* u trećim zemljama i međunarodnim organizacijama koji mogu biti od uticaja na akt za sprovođenje (čl. 45 st. 4 OUZP). Ukoliko Komisija ustanovi da *adekvatan nivo zaštite podataka više ne postoji*, ona je u obavezi da aktima za sprovođenje *stavi*

[235] Ažurirana lista trećih zemalja sa adekvatnim nivoom zaštite podataka može se pronaći na veb stranici Evropske Komisije https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

van snage, izmeni ili suspenduje odluku adekvatnosti (čl. 45 st. 5 OUZP). U slučaju razloga krajnje hitnosti Komisija donosi akte za sprovođenje koji odmah počinju da se primenjuju. Uz to Komisija treba da započinje *savetovanje* s trećom zemljom ili međunarodnom organizacijom *radi popravljanja stanja* koje je dovelo do stavljanja van snage ili izmene ili suspenzije odluke o adekvatnosti (čl. 45 st. 6 OUZP).

Treba istaći da *ukoliko Komisija stavi van snage ili izmeni ili suspenduje odluku o adekvatnosti*, to *ne dira u dopuštenost ostalih pravnih osnova za prenos podataka* u treće zemlje shodno čl. 46 – 49 OUZP (čl. 45 st. 7 OUZP) .

Komisija je u obavezi da u Službenom listu Evropske unije objavljuje *spisak svih trećih zemalja*, teritorija i konkretnih sektora unutar treće zemlje i međunarodnih organizacija u vezi s kojima je donela odluku da *obezbeđuju,* odnosno da *više ne obezbeđuju adekvatan nivo zaštite* (čl. 45 st. 8 OUZP).[236]

2. Prenos na osnovu adekvatnih zaštitnih mera (čl. 46 OUZP)

Preduzimanje adekvatnih zaštitnih mera takođe može biti jedan od osnova za prenos podataka u treće zemlje. Pored adekvatnih zaštitnih mera *neophodno je i to, da pojedinci imaju garantovana u trećoj zemlji da su njihova prava izvršiva kao i delotvorna pravna sredstva* (čl. 46 st. 1 OUZP).

Adekvatne zaštitne mere moraju da se odnose na *pridržavanje sa opštim načelima obrade podataka* kao *i sa principima ugrađene i podrazumevane zaštite podataka* (U.t.r. 108 OUZP).

Adekvatne zaštitne mere mogu da budu obezbeđene bez odluke nadzornog organa na neki od sledećih načina (čl. 46 st. 2 OUZP):

- ✓ *pravno obavezujućim i izvršnim dokumentom* između organa javne vlasti ili javnih tela (ne važi za privatan sektor);
  Prenose podataka mogu da obavljaju organi vlasti ili tela sa javnim ovlašćenjima ili tela u trećim zemljama ili pri međunarodnim organizacijama sa odgovarajućim dužnostima ili funkcijama, između ostalog na osnovu odredaba koje se uključuju u *administrativne aranžmane*, kao što je memorandum o razumevanju, kojima se obezbeđuju ostvariva i efikasna prava za lica na koje se podaci odnose. Kada se mere zaštite predviđaju u administrativnim aranžmanima koji nisu pravno obavezujući, mora da se dobije odobrenje nadležnog nadzornog organa (U.t.r. 108 OUZP).
- ✓ *obavezujućim korporativnim pravilima* (čl. 47 OUZP) - (ne važi za javni sektor);
- ✓ *standardnim klauzulama* o zaštiti podataka koje donosi Komisija (čl. 93 st. 2 OUZP);
- ✓ *standardnim klauzulama* o zaštiti podataka koje donosi nadzorni organ i koje Komisija odobrava (čl. 93 st. 2 OUZP);

[236] *Ibidem*, str. 257, 261, 262.

- ✓ *odobrenim kodeksom ponašanja* (čl. 40 OUZP), zajedno sa obavezujućim i izvršnim obavezama rukovaoca ili obrađivača u trećoj zemlji za primenu odgovarajućih zaštitnih mera, između ostalog i u pogledu prava lica na koja se podaci odnose;
  Radi se o pravilima ponašanja koja usvajaju interesne grupacije, sindikati, koji preciziraju specifičnosti određene branše u pogledu obrade podatka. Pritom je moguće da ovakva pravila ponašanja obavežu rukovaoca ili obrađivača na njihovo poštovanje.[237]
- ✓ *odobrenim mehanizmom sertifikacije* (čl. 42 OUZP), zajedno sa obavezujućim i izvršnim obavezama rukovaoca ili obrađivača u trećoj zemlji za primenu odgovarajućih zaštitnih mera, između ostalog i u pogledu prava lica na koja se podaci odnose.[238]

Adekvatne zaštitne mere mogu da budu obezbeđene i *na osnovu odluke nadzornog organa* na neki od sledećih načina (čl. 46 st. 3 OUZP):

- ✓ *ugovornim klauzulama* između rukovaoca ili obrađivača i rukovaoca, obrađivača ili korisnika podataka o ličnosti u trećoj zemlji ili međunarodnoj organizaciji;
- ✓ odredbama koje se unose u *administrativne dogovore* između organa javne vlasti ili javnih tela i koja sadrže izvršna i efektivna prava lica na koja se podaci odnose.
  Prenose podataka mogu da obavljaju organi vlasti ili tela sa javnim ovlašćenjima ili tela u trećim zemljama ili pri međunarodnim organizacijama sa odgovarajućim dužnostima ili funkcijama, između ostalog na osnovu odredaba koje se uključuju u *administrativne aranžmane*, kao što je memorandum o razumevanju, kojima se obezbeđuju ostvariva i efikasna prava za lica na koje se podaci odnose. Kada se mere zaštite predviđaju u administrativnim aranžmanima koji nisu pravno obavezujući, mora da se dobije odobrenje nadležnog nadzornog organa (U.t.r. 108 OUZP).

Već donete *odluke pre stupanja OUZP vezane za standardne klauzule* iz razloga pravne sigurnosti *nastavljaju da se primenjuju* (čl. 46 st. 5 OUZP). *Isto važi i za ostala odobrenja prenosa podataka* shodno odlukama nadzornih organa, osim ako ih nadzorni organ ne izmeni, zameni ili stavi izvan snage ako je potrebno.[239]

Standardne klauzule koje je Komisija usvojila, omogućavaju i po OUZP uslovno (pošto je moguće da postoji specifična implementacija zavisno od države članice EU)

[237] Thomas Strohmaier, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 245.

[238] Trenutno na nivou EU postoji jedan pečat kvaliteta EuroPriSe (The European Privacy Seal https://www.european-privacy-seal.eu/EPS-en/Home). Ovim pečatom tj. garantom kvaliteta moguća je sertifikacija za IT proizvode i IT-usluge kao i veb stranice na osnovu standarda zaštite podataka. Lista sertifikovanih kompanija je takođe javno dostupna https://www.european-privacy-seal.eu/EPS-en/awarded-seals.

[239] Rainer Knyirm, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 263, 265, 268.

slobodan prenos za organizacije, koje iz potpišu.[240] To su 2 varijante, koje i po stupanju OUZP mogu da se koriste. Mogu se koristiti ili varijanta 1 ili varijanta 2. Ovi ugovori se ne mogu spajati i moraju biti u izvornom obliku, u kakvom ga je Komisija usvojila.

Varijanta 1 je namenjena za prenos podataka ka rukovaocima iz trećih zemalja (može se naći na stranici https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32001D0497&from=IT)

Varijanta 2 je namenjena pre svega za obrađivače iz trećih zemalja (može se naći na stranici https:// eur-lex. europa. eu/ legal-content/ DE/ ALL/?uri=celex%3A32010D0087). Treba imati u vidu da ova varijanta važi ako obrađivač iz treće zemlje želi da uključi dalje obrađivače iz trećih zemalja (U.t.r. 23 odluke Komisije). To je pre svega situacija sedište u EU rukovalac-sedište van EU obrađivač-sedište van EU sub-obrađivač.

Varijanta 2 ne važi za situaciju: sedište u EU rukovalac-sedište u EU obrađivač-sedište van EU sub-obrađivač.

Kao pravni osnov može se iskoristiti u navedenoj situaciji:

- ✓ *Direktan ugovor* između rukovaoca sa sedištem u EU i sa sub-orađivačem koji ima sedište van EU;
- ✓ *Jasan nalog* od strane rukovaoca sa sedištem u EU za obrađivača sa sedištem u EU da zaključi ugovor na osnovu standardnih klauzula po varijanti 2 sa sub-obrađivačem koji ima sedište van EU;
- ✓ *Ad hok ugovor* koji mora da sadrži načela zaštite podataka i garancije iz standardnih ugovornih klauzula.[241]

Varijanta 2 ne rešava sledeću situaciju: sedište u EU rukovalac-sedište van EU obrađivač-sedište van EU sub-obrađivač. U tom slučaju ostavljeno je ugovornim stranama da odluče da li će dozvoliti generalno uključivanje sub-obrađivača ili će biti potrebno odobrenje za uključivanje svakog pojedinačnog sub-obrađivača.[242]

3. Prenos podataka bez odluke o adekvatnosti ili odgovarajućih zaštitnih mera uključujući i obavezujuća korporativna pravila (čl. 49 OUZP)

Prenos podataka u treću zemlju može biti dopušten i u slučaju da ne postoje ni odluka o adekvatnosti ni odgovarajuće zaštitne mere uključujući i obavezujuća korporativna pravila.

[240] Tako je u Austriji potrebno da ove ugovore potvrdi nadzorni organ.

[241] Artikel-29-Datenschutzgruppe, Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG, 12.07.2010., 00070/2010/DE, WP 176, str. 3, 4, 5.

[242] Takođe postoje i alternativne standardne klauzule koje je Komisija usvojila. Postoje takođe 2 varijante ovih klauzula. Mogu se pronaći na stranici https://iccwbo.org/publication/icc-alternative-standard-contractual-clauses-for-the-transfer-of-personal-data-from-the-eu-to-third-countries/

Za dopuštenost prenosa podataka treću zemlju u navedenom slučaju neophodno je ispuniti sledeće uslove:

- ✓ lice na koje se podaci odnose je *izričito pristalo na predloženi prenos* nakon što je upoznato sa mogućim rizicima takvih prenosa za lica na koja se podaci odnose zbog nepostojanja odluke o adekvatnosti i odgovarajućih zaštitnih mera;
- ✓ prenos je potreban za *izvršenje ugovora* između lica na koje se podaci odnose i rukovaoca ili primenu predugovornih mera na zahtev lica na koje se podaci odnose;
- ✓ prenos je potreban *radi sklapanja ili izvršenja ugovora* sklopljenog u interesu lica na koje se podaci odnose između rukovaoca i drugog fizičkog ili pravnog lica;
- ✓ prenos je potreban iz važnih razloga *javnog interesa*;
- ✓ prenos je potreban za *postavljanje, ostvarivanje ili odbranu pravnih zahteva*;
- ✓ prenos je potreban za *zaštitu životno važnih interesa* lica na koje se podaci odnose ili drugih lica ako *lice* na koje se podaci odnose *fizički ili pravno nije sposoban da dâ pristanak*;
- ✓ prenos se vrši iz *registra* koji prema pravu Unije ili pravu države članice služi *za pružanje informacija javnosti* i koji je dostupan za uvid javnosti ili bilo kom licu koje može da dokaže postojanje *legitimnog interesa*, ali samo ako su ispunjeni uslovi propisani pravom Unije ili pravom države članice za uvid u tom posebnom slučaju.
- ✓ Kao što se može primetiti navedeni uslovi za prenos podataka u treće zemlje postavljeni su alternativno. Pored toga oni sadržinski u mnogome odgovaraju opštim uslovima dopuštenosti obrade podataka iz čl. 6 st. 1 OUZP.

Zakonski osnovi a, b i c *ne primenjuju se na rukovaoce ili obrađivače u obavljanju javne vlasti* (čl. 49 st. 3 OUZP). Tako da su on primenjivi samo u privatnom sektoru!

4. Poseban pravni osnov prenosa podataka (čl. 49 OUZP poslednji pasus)

Prenos podataka u treću zemlju može biti dopušten i u slučaju da ne postoje ni odluka o adekvatnosti ni odgovarajuće zaštitne mere uključujući i obavezujuća korporativna pravila, ali takođe ni ispunjeni uslovi iz čl. 49 OUZP.

U čl. 49 OUZP poslednji pasus OUZP je predvideo još jednu mogućnost za prenos u treće zemlje, ukoliko su *kumulativno ispunjeni sledeći kriterijumi*:

- ✓ ako se prenos ne ponavlja;
- ✓ ako se tiče samo ograničenog broja lica na koja se podaci odnose;
- ✓ ako je neophodan radi ostvarivanja nužnih legitimnih interesa rukovaoca nad

kojima ne preovlađuju interesi ili prava i slobode lica na koja se podaci odnose, a rukovalac je procenio sve okolnosti prenosa podataka i na osnovu te procene je predvideo odgovarajuće zaštitne mere u pogledu zaštite podataka o ličnosti;
- ✓ ako je o tome obavestio nadzorni organ;
- ✓ ako je rukovalac pružio informacije iz člana 13. i 14 o prenosu i o nužnim legitimnim interesima licu na koje se podaci odnose.

Rukovalac ili obrađivač su u *obavezi da u evidenciji aktivnosti obrade* (čl. 30 OUZP) *dokumentuju procenu i odgovarajuće zaštitne mere* (čl. 49 st. 6 OUZP), ukoliko koriste ovaj zakonski osnov.

Ovaj zakonski osnov *ne primenjuje se na rukovaoce ili obrađivače u obavljanju javne vlasti* (čl. 49 st. 3 OUZP). Tako da je on primenjiv samo u privatnom sektoru!

14.1. Obavezujuća korporativna pravila (čl. 47 OUZP)

Obavezujuća korporativna pravila (eng. *Binding Corporate Rules*) su postojala kao pravni instrument i po Direktivi o zaštiti podataka iz 95. godine. Ovaj pravni instrument omogućava *multinacionalnim kompanijama da regulišu pregogranične prenose podataka* u okviru povezanih preduzeća, koja se nalaze u velikom broju zemlja. Na ovaj način je moguće internim obavezujućim korporativnim pravilima obavezati se na poštovanje pravila zaštite podataka. Ovaj instrument je stoga *od značaja za prenose u tzv. treće zemlje*, koje nemaju adekvatan nivo zaštite podataka kao i za prenose podataka multinacionalnih kompanija u okviru koncerna.[243]

Obavezujuća korporativna pravila *odobrava nadležni nadzorni organ* u skladu sa mehanizmom konzistentnosti (čl. 63 OUZP). Pritom nadzorni organ procenuje sledeće uslove (čl. 49 st. 1 OUZP):

- ✓ da li se pravno obavezujuća primenjuju *na svakog zainteresovanog člana određene grupe povezanih društava ili grupe preduzeća* koja obavljaju zajedničku privrednu delatnost, kao i njihove zaposlene, i da li ih svaki od tih članova izvršava; i
- ✓ da li se *licima na koja se podaci odnose izričito daju izvršna prava* u vezi sa obradom njihovih podataka o ličnosti; i
- ✓ ispunjavanje posebnih zahteva vezanih za sama obavezujuća korporativna pravila.

[243] Lista kompanija kojima su odobrena obavezujuća korporativna pravila, može se pogledati na sledećem linku https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en pod nazivom „BCR overview until 25th May 2018“.

Posebni zahtevi koji se odnose na sama obavezujuća korporativna pravila su (čl. 49 st. 2 OUZP):

- ✓ struktura i podaci za kontakt grupe povezanih društava ili grupe preduzeća koja obavljaju zajedničku privrednu delatnost i svakog od njenih članova;
- ✓ prenosi podataka ili skupovi prenosa, uz navođenje kategorije podataka o ličnosti, vrste obrade i njene svrhe, vrste lica na koja se podaci odnose i određenja konkretne treće zemlje, odnosno zemalja;[244]
- ✓ pravno obavezujuća priroda pravila o zaštiti podataka, kako interno, tako i eksterno;[245]
- ✓ primena opštih načela zaštite podataka, a posebno ograničavanja svrhe, korišćenja najmanjeg mogućeg obima podataka, ograničenog roka čuvanja, kvaliteta podataka, ugrađene i podrazumevane zaštite podataka, osnova obrade, obrade posebnih kategorija podataka o ličnosti, mera za postizanje bezbednosti podataka i uslove u vezi s daljim prenosom telima koja nisu obavezana obavezujućim korporativnim pravilima;[246]
- ✓ prava lica na koja se podaci odnose u vezi s obradom i načine za ostvarenje tih prava, uključujući i pravo da se na njih ne primenjuju odluke koje se zasnivaju isključivo na automatskoj obradi, što uključuje i profilisanje u skladu sa članom 22, pravo na pritužbu nadležnom nadzornom organu i nadležnim sudovima država članica u skladu sa članom 79. i pravo na sudsku zaštitu, a u odgovarajućim slučajevima i pravo na naknadu za kršenje obavezujućih korporativnih pravila;
- ✓ prihvatanje odgovornosti rukovaoca ili obrađivača sa sedištem na teritoriji države članice za sva kršenja obavezujućih korporativnih pravila od strane bilo kog člana koji nema sedište u Uniji; rukovalac ili obrađivač je u celini ili delimično izuzet od ove odgovornosti samo ako dokaže da taj član nije odgovoran za događaj koji je prouzrokovao štetu;
- ✓ način na koji se licima na koja se podaci odnose pored informacija iz člana 13. i 14. pružaju informacije o obavezujućim korporativnim pravilima, posebno o odredbama iz tačaka (d), (e) i (f) ovog stava;
- ✓ zadaci svakog ovlašćenog lica za zaštitu podataka imenovanog u skladu sa članom 37. ili bilo kog drugog lica ili subjekta odgovornog za praćenje usklađenosti s obavezujućim korporativnim pravilima u grupi povezanih društava ili grupi preduzeća koja obavljaju zajedničku privrednu delatnost, kao i za praćenje osposobljavanja i postupanja po pritužbama;
- ✓ postupci povodom pritužbi;[247]

[244] Ovo ne znači da su dopušteni svi prenosi, već da se i dalje prenosi obavljaju u skladu sa svrhom i da se radi o osnovnoj delatnosti. Slično kao kod standardnih klauzula. Tako da se moraju opisati konkretne svrhe i kategorije podataka o ličnosti.

[245] Rainer Knyirm, *Datenschutz-Grundverordnung*, Knyrim, 2016., str. 270.

[246] Radi se o ispunjavanju načela zaštite podataka (čl. 5 OUZP) i dokazivanju istih (čl. 24 OUZP).

[247] Ovo se odnosi na interni postupak u slučaju da se pojedinci žale u vezi sa prenosom podataka u treće zemlje po osnovu obavezujućih korporativnih pravila.

- ✓ mehanizmi unutar grupe povezanih društava ili grupe preduzeća koja obavljaju zajedničku privrednu delatnost kojima se obezbeđuje provera poštovanja obavezujućih korporativnih pravila. Takvi mehanizmi uključuju revizije zaštite podataka i metode za obezbeđivanje korektivnih mera za zaštitu prava lica na koja se podaci odnose. Rezultate takve provere potrebno je saopštiti licu ili subjektu iz tačke (h) i upravnom odboru društva u kontrolišućem položaju u grupi povezanih društava ili grupi preduzeća koja obavljaju zajedničku privrednu delatnost, a na zahtev ih je potrebno staviti na raspolaganje i nadležnom nadzornom organu;[248]
- ✓ mehanizme za obaveštavanje i vođenje evidencije o promenama pravila i obaveštavanje nadzornog organa o tim promenama;
- ✓ mehanizam saradnje sa nadzornim organom radi obezbeđivanja usklađenosti svakog člana grupe povezanih društava ili grupe preduzeća koja obavljaju zajedničku privrednu delatnost, pre svega tako što se nadzornom organu stavljaju na raspolaganje rezultati provera mera iz tačke (j);
- ✓ mehanizme za obaveštavanje nadležnog nadzornog organa o bilo kakvim pravnim obavezama koje se na člana grupe povezanih društava ili grupe preduzeća koja obavljaju zajedničku privrednu delatnost primenjuju u trećoj zemlji, a koje bi mogle da imaju značajan negativan uticaj na garancije sadržane u obavezujućim korporativnim pravilima; i
- ✓ odgovarajuće osposobljavanje iz oblasti zaštite podataka za osoblje koje ima stalan ili redovan pristup podacima o ličnosti.

Komisija može da odredi *format i postupke* (u skladu sa postupkom pregleda iz čl. 93 st. 2 OUZP) razmene informacija između rukovalaca, obrađivača i nadzornih organa za obavezujuća korporativna pravila (čl. 47 st. 3 OUZP).

[248] Radi se o internim kontrolnim mehanizmima radi obezbeđivanja poštovanja obavezujućih korporativnih pravila. To može biti interni kontrolni sistem ili interni/eksterni audit.

15. ZAKLJUČAK

Nova pravila o zaštiti podataka u evropskom pravu predstavljaju izuzetan napredak u oblast zaštite podataka i možda jedan od najznačajnijih propisa ikada donetih koji je vezan za informacione tehnologije.

OUZP nam donosi najviše standarde zaštite podataka, koji su u velikoj meri i do sada bili proklamovani, ali nisu do sada nikada na ovakav način primenjivani. Područje primene OUZP-a je globalno i faktički obuhvata ceo svet. Ovaj propis primenjuje se na kompanije koje prikupljaju i obrađuju podatke o ličnosti kada se njihovo predstavništvo nalazi u EU, ali u određenim slučajevima i kada se njihovo predstavništvo nalazi izvan EU.

OUZP prati drakonski sistem sankcija, čije nepoštovanje može u potpunosti onemogućiti poslovanje čak i najvećih kompanija. Sankcije mogu dostići milione, pa čak u nekim ekstremnim slučajevima i milijarde evra. Pojedinci dobijaju nova prava u zaštiti njihovih podataka, ali isto tako i mehanizme zaštite tih prava. Nacionalna zakonodavstva predviđaju tri vrste odgovornosti za kršenje odredaba zaštite podataka o ličnosti. To su prekršajna odgovornost pravnih i fizičkih lica, građanska odgovornost pravnih i fizičkih lica, kada dođe do materijalne ili nematerijalne štete, i krivična odgovornost fizičkih lica za počinjena krivična dela shodno nacionalnim zakonodavstvima.

Usaglašavanje sa OUZP zahteva od organizacija koje obrađuju lične podatake preduzimanje odgovarajućih organizacionih, tehničkih i praktičnih koraka. Prvi od tih koraka je svakako detaljno upoznavanje sa odredbama OUZP i njenom praktičnom primenom. Razumevanje načela, standarda, instituta i načina efikasne zaštite ličnih podataka u okviru baza podataka i virtuelnog okruženja preduslov je uspešne primene OUZP-a.

Opštom Uredbom o zaštiti podataka stvoren je složen sistem zaštite podataka koji ima veliki uticaj na promenu shvatanja o značaju zaštite podataka u čitavom svetu. Sve veća ugroženost osnovnih ljudskih prava, među kojima i prava na privatnost, od strane, pre svega velikih svetskih kompanija, ali i država, manjih kompanija, i pojedinaca, prouzrokovala je traženje što adekvatnijeg odgovora. Taj odgovor se može naći ne samo u usaglašenosti sa Opštom uredbom o zaštiti podataka nego i u rečima profesora Renea Majerhofera:

"Znanje nastaje iz sirovih podataka i algoritama. Uporediti podatke sa naftom ili zlatom je zabluda, pošto se podaci sa marginalnim troškovima mogu kopirati. Stoga će budućnost biti drugačija nego sa fizičkim resursima - neće biti nedostatka resursa, već će u budućnosti biti odlučujuća kontrola kopija podataka."

16. LITERATURA

Bainbridge David, *Introduction to Computer Law*, Longman, 2000.

Bergauer Christian, *Datenschutz-Grundverordnung*, Knyrim, izdato 2016.

Diligenski Andrej, Prlja Dragan, *Fejsbuk, zaštita podataka i sudska praksa*, Institut za uporedno pravo Beograd, 2018.

Dimitrijević Predrag, *Pravo informacione tehnologije*, SVEN, Niš, 2010.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201 , 31/07/2002.*

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal L 105 , 13/04/2006.*

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal L 337 , 18/12/2009.

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, *Official Journal L 337 , 18/12/2009*.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995.

Đukić Dejan, *Zaštita podataka o ličnosti sa osvrtom na novo zakonodavstvo EU u ovoj oblasti*, Pravni zapisi, Pravni fakultet Univerziteta Union, Beograd, br. 1/2017.

Fink Simon, *Datenschutz zwischen Staat und Markt (Die „Safe Harbor"-Lösung als Ergebnis einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie)*, UNIVERSITÄT KONSTANZ, 2002, Magisterarbeit.

Haidinger Viktoria, *Datenschutz-Grundverordnung*, Knyrim, 2016.

Hladjk Jörg, *Datenschutz-Grundverordnung*, Knyrim, 2016.

Hoeren Thomas, Big Data and the Ownership in Data: Recent Developments in Europe, European Intellectual Property Review 12/2014.

Illibauer Ursula, *Datenschutz-Grundverordnung*, Knyrim, 2016.

Jahnel Dietmar, Handbuch Datenschutzrecht, Jan Sramek Verlag, 2010.

Kastelitz Markus, *Datenschutz-Grundverordnung*, Knyrim, 2016.

Lambert Paul, *Understanding the New European Data Protection Rules*, CRC Press, Boca Raton, 2018.

Leenes Ronald, et al, editors, *Data Protection and Privacy: (In) visibilities and Infrastructures*, Springer, 2017.

Lilić Stevan, *Pravo, informatička tehnologija i zaštita podataka*, Anali Pravnog fakulteta, br. 2-3/1989Prlja Dragan, Reljanović Mario, *Pravna informatika*, Beograd, Službeni glasnik, 2010.

Popesku Dragica, *Zaštita prva privatnosti i njegove sfere*, Strani pravni život, br. 1/2016.

Popović Dušan, Jovanović Marko, Pravo interneta: odabrane teme, Univerzitet u Beogradu - Pravni fakultet, Beograd, 2017.

Prlja Sanja, *Pravo na zaštitu ličnih podataka u EU*, Strani pravni život, Institut za uporedno pravo, Beograd, br. 1/2018.

Regulation 2016/679 of the European Parliament and of the Council of 7 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, p. 1–88.

Rosenthal Simone, Bonstein Felix, *Wegradiert, DSGVO – Datenlöschung*, EU-DSGVO konkret, IX Magazin für professionelle Informationsrechnik, 2018.

Savet Evrope, *Konvencija o zaštiti ljudskih prava i osnovnih sloboda*, Rim, 1950, http:// www. echr. coe. int/ NR/rdonlyres/EA13181C-D74A-47F9-A4E5-8A3AF5092938/0/ Convention_BOS.pdf, 4.3.2013.

Savović Miodrag, *Internet i zaštita prava na privatnost*, u Dragan Todorović, Dalibor Petrović, Dragan Prlja, "Internet i društvo", Srpsko sociološko društvo, Univerzitet u Nišu Filozofski fakultet, Institut za uporedno pravo, Niš, 2014.

Schafer Arthur, *Privacy - A Philosophical Overview*, *Aspects of Privacy Law*, Edited by Dale Gibson, Toronto, 1980.

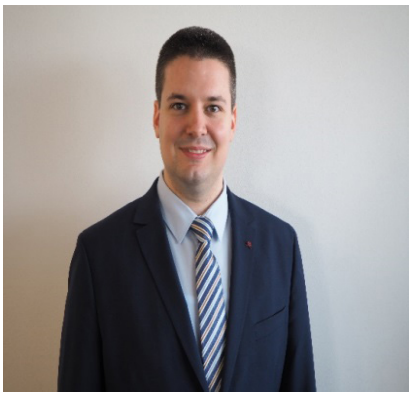
Steinmaurer Klaus M., *Datenschutz-Grundverordnung*, Knyrim, 2016.

Vodinelić Vladimir, *Obrada podataka i zaštita ličnosti*, Anali Pravnog fakulteta, br. 2-3/1989

Vodinelić Vladimir, *Pravo zaštite ličnih podataka*, u Nebojša Šarkić, i dr. "Pravo informacionih tehnologija", Pravni fakultet Univerziteta Union, 2007

Voigt Paul, Vvon dem Bussche Axel, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017.

Warren Samuel, Brandais Louis, *The Right to be Left Alone*, Harvard Law Review, 1890.



ANDREJ DILIGENSKI

Andrej Diligenski rođen je u Beogradu 1984. godine, gde je diplomirao na Pravnom fakultetu Univerziteta u Beogradu na međunarodnopravnom smeru. Specijalističke master studije je završio u Beču u oblasti informatičkog prava i prava informacionih tehnologija na temu „Implemtentacija elektronske uprave - poređenje Austrije i Srbije" („Umsetzung von E-Government" - Ein Vergleich zwischen Österreich und Serbien).Trenutno radi na odbrani doktorske disertacije na Pravnom fakultetu u Beču na temu „Zaštita podataka u telekomunikacionom pravu Crne Gore" (Datenschutz im Telekommunikationsrecht Montenegros).

Sertifikovan je od austrijskog sertifikacionog tela ARGE DATEN i austrijskog univerziteta Donau Uni Krems kao poverenik za zaštitu podataka. Pored toga je i sertifikovan menadžer za informacionu sigurnost (information security manager) po svetskom standardu ISO 27001 od austrijskog sertifikacionog tela CIS.

Zaposlen je kao menadžer za zaštitu podataka firme SVD Büromanagement GmbH u Beču.

Spoljni saradnik je Instituta za uporedno pravo u Beogradu. Objavio je više naučnih radova i blogova između ostalih „Zaštita autorskih prava u digitalnom svetu", „Pravni aspekti neutralnosti internet mreže", „Organizovani kriminal i digitalna forenzika", „Zaštita podataka kod mergers & acquisitions", „Religija, politika i pravo u sajber svetu", itd.

E-mail: andrej84_4@hotmail.com

DRAGAN PRLJA

Dragan Prlja rođen je u Ostojićevu 1959. godine, a diplomirao je, magistrirao i doktorirao na Pravnom fakultetu Univerziteta u Beogradu na međunarodnopravnom smeru kod profesora Vojina Dimitrijevića.

Tokom karijere bavio se istraživačkim poslovima u Institutu ekonomskih nauka u Beogradu, Institutu za međunarodnu politiku i privredu u Beogradu, i Institutu za uporedno pravo u Beogradu.

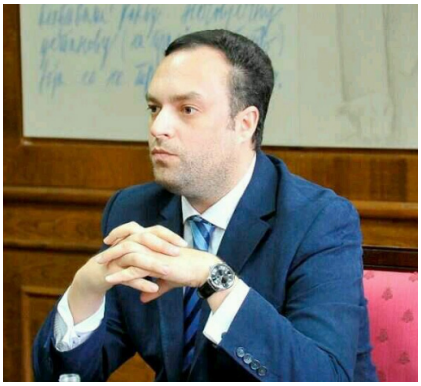
Jedan je od osnivača nastavnog predmeta pravna informatika na više fakulteta i univerziteta. Predavao je pravnu informatiku na Pravnom fakultetu Univerziteta u Beogradu, Pravnom fakultetu Univerziteta Crne Gore u Podgorici, i Pravnom fakultetu Univerziteta Union u Beogradu.

Bio je osnivač više nevladinih organizacija: Jugoslovenskog društva za pravnu informatiku, Jugoslovenskog komiteta za ljudska prava, i drugih.

Učestvovao je u realizaciji većeg broja nacionalnih i međunarodnih projekata iz oblasti prava i informatike.

Objavio je samostalno, ili kao koautor tridesetak knjiga: Pravna informatika, Fejsbuk, zaštita podataka i sudska praksa, Digitalna forenzika, Internet i pravo, itd. i preko sto članaka iz oblasti prava i informatike u časopisima i zbornicima u zemlji i inostranstvu.

E-mail: dprlja@gmail.com



DRAŽEN CEROVIĆ

Dražen Cerović je rođen 2. avgusta 1975. godine u Titogradu.

Diplomirao je na Pravnom fakultetu Univerziteta Crne Gore, 1999. godine, kao jedan od najboljih studenata u generaciji. Postdiplomske studije je završio na Pravnom fakultetu Univerziteta u Beogradu, na kome je stekao naučno zvanje magistra pravnih nauka 2003. godine. Magistarski rad, pod nazivom "Upravna stvar i ustavna žalba", odbranio je *Summa Cum Laude / With Highest Honor* (sa odlikom). Doktorsku tezu pod nazivom "Parlamentarna kontrola javne uprave, takođe je odbranio *Summa Cum Laude / With Highest Honor (*sa odlikom) 2007. godine.

Prof. dr Dražen Cerović je na Univerzitetu Crne Gore izabran u sva dosadašnja zvanja. Za asistenta izabran je 2000. godine, u zvanje docenta 2009. godine, a u zvanje vanrednog profesora 2014. godine. Predaje Upravno pravo, Policijsko pravo i Bezbjednosni menadžment, na Pravnom fakultetu Univerziteta Crne Gore.

Autor je velikog broja monografija, članaka i publikacija iz naučnog i društvenog života. Govori engleski i ruski jezik. Uže oblasti interesovanja: Parlamentarna kontrola javne uprave, Ustavna zaštita građanskih prava i sloboda, Upravno pravo Evropske unije, Principi Evropskog administrativnog prostora, Ustavno uređenje evropskih država, Upravljanje bezbjednosnim sektorom i reforma službi bezbjednosti, i Zaštita podataka.

E-mail: drazen.cerovic@gmail.com

CIP - Каталогизација у публикацији -
Народна библиотека Србије, Београд

342.738(4-672EU)
342.727(4-672EU)
004.056.5:34(4-672EU)

ДИЛИГЕНСКИ, Андреј, 1984-
Pravo zaštite podataka GDPR / Andrej Diligenski, Dragan Prlja, Dražen Cerović. - Beograd : Institut za uporedno pravo, 2018 (Beograd : Planeta print). - 221 str. ; 24 cm

Slike autora. - Tiraž 500. - [O autorima]: str. 219-221. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 217-218.

ISBN 978-86-80186-42-9
1. Прља, Драган, 1959- [аутор] 2. Церовић, Дражен, 1979- [аутор]
a) Општа уредба о заштити података личности ЕУ b) Право на заштиту података о личности - Европска унија COBISS.SR-ID 272151820