Utjecaj Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća Europske unije na upravljanje i zaštitu osobnih podataka u zdravstvenom sustavu Republike Hrvatske

Nola Fuchs, Petra

Professional thesis / Završni specijalistički

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, School of Medicine / Sveučilište u Zagrebu, Medicinski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:105:368574

SVEUČILIŠTE U ZAGREBU

MEDICINSKI FAKULTET

Petra Nola Fuchs

Utjecaj Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća Europske unije na upravljanje i zaštitu osobnih podataka u zdravstvenom sustavu Republike Hrvatske

Završni specijalistički rad

Zagreb, 2022. godina

Ovaj diplomski rad izrađen je u Stomatološkoj poliklinici Zagreb pod vodstvom prof. dr. sc. Stjepana Oreškovića i predan je na ocjenu u akademskoj godini 2020.

Redni broj rada: _____

Sadržaj

1. Uvod

UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), u(u daljnjem tekstu Uredba) predstavlja velik iskorak u području zaštite osobnih podatka i informacijske sigurnosti [1] [2].
Dosadašnji pravni okvir koji je bio definiran nacionalnim zakonodavstvima i Direktivom 95/46/EC [3] (koja se stavlja van snage) uistinu se pokazao nedovoljnim kako bi se uredilo virtualno okruženje i zaštita prava građana EU u pogledu obrade njihovih osobnih podataka. Ključna pretpostavka razvoja suvremene digitalne ekonomije temelji se na ubrzanom razvoju informacijskih i komunikacijskih tehnologija, istodobno stvarajući nove izazove i ugroze privatnosti i zaštite osobnih podataka.

Obrada podataka, osobito obrada osobnih podataka, novi IT alati i digitalno tržište, razvilo je potrebu za povećanjem zaštite privatnosti novih digitalnih proizvoda i usluga stoga je stav o uvođenju Uredbe u obaveznu praksu opravdan.

Sama Uredba predstavlja bitan napredak u području zaštite osobnih podataka budući da se s njim osigurava ujednačeno i jednoobrazno postupanje nadzornih tijela za zaštitu osobnih podataka, što će imati za posljedicu jednostavniju i jednaku zaštitu prava svih pojedinaca u Europskoj uniji i to na način da sam pojam “Uredbe” znači da se izravno primjenjuje u zakonodavni okvir zemalja članica (izuzev u nekolicini pojmova koji se ostavljeni za razradu u nacionalnim zakonodavstvima) za razliku od do sada važeće “Direktive” koja je predstavljala “samo” smjernicu djelovanja.

Također, uvode se nove i pojednostavljuju se neke već postojeće definicije, određuju i definiraju novi pojmovi koji do sada nisu bili zakonski definirani, kao biometrijski i genetski podaci, preciznije opisuju postojeći pojmovi, jačaju prava ispitanika te se smanjuju i pojednostavljuju pojedine administrativne obveze voditelja zbirke osobnih podataka, jačaju nadzorne ovlasti te mogućnost izricanja kazni od strane tijela za zaštitu osobnih podataka.
Europska komisija objavila je pak rezultate posebnog istraživanja Eurobarometra o zaštiti podataka [4]. Rezultati pokazuju da su Europljani relativno dobro upoznati s novim pravilima

o zaštiti podataka, svojim pravima i postojanjem nacionalnih tijela za zaštitu podataka, kojima se mogu obratiti ako su im prava prekršena.

Rezultati Eurobarometra [4] na temelju mišljenja 27 000 Europljana pokazuju da:

- 73% ispitanika zna za barem jedno od šest prava navedenih u anketi koja su zajamčena Općom uredbom o zaštiti podataka.
- građani su najbolje upoznati s pravom na pristup osobnim podacima (65 %),
- pravom na ispravak podataka ako su netočni (61%),
- pravom na odbijanje izravnog marketinga (59%) i
- pravom na brisanje osobnih podataka (57%).
- 67% ispitanika upoznato je s Općom uredbom o zaštiti podataka, a
- 57% zna koja su nacionalna tijela nadležna za zaštitu podataka.

Rezultati pokazuju i da je zaštita podataka važno pitanje jer 62% ispitanika smatra da nema potpunu kontrolu nad osobnim podacima na internetu [4].
Nameće se zaključak da je Opća uredba o zaštiti podataka jedinstven skup pravila koji se temelji na zajedničkom pristupu EU-a zaštiti osobnih podataka te se izravno primjenjuje u državama članicama. Ona jača povjerenje tako što pojedincima daje kontrolu nad osobnim podacima, a istovremeno jamči slobodan protok osobnih podataka među državama članicama EU-a. Zaštita osobnih podataka temeljno je pravo u Europskoj uniji [5].

Od 25.5.2018. gotovo su sve države članice prilagodile svoje nacionalno zakonodavstvo njezinim odredbama, što stoji i u priopćenju Komisije. Nacionalna tijela za zaštitu podataka nadležna su za provedbu tih novih pravila i bolje koordiniraju svoj rad zahvaljujući novim mehanizmima suradnje i Europskom odboru za zaštitu podataka. Ona izdaju smjernice o ključnim aspektima Opće uredbe o zaštiti podataka koje podupiru provedbu novih pravila.
Dakle, donošenje Uredbe prvenstveno predstavlja pravni okvir kojim je EU odlučila zaštiti privatnost svojih građana i povećati kontrolu nad obradom osobnih podataka građana uz uvođenje zakonske obveze procjene učinka na zaštitu podataka. Također, ova Uredba JE postrožila dodatno i obradu posebnih kategorija podataka u području "e-zdravstva", [6] [7] [8], te se samim time uistinu očekuje potrebna edukacije i usklađivanja s novom Uredbom.
Kod kibernetičkog kriminala ovim se dobiva dodatna zaštita jer su se postrožile i mjere zaštite sukladno osjetljivosti osobnih podataka – s naglaskom na posebno osjetljive podatke

(maloljetne osobe, medicinski podaci, isl.) Propisana je gornja granica sankcija i upravnih novčanih kazni te je prepušteno nacionalnim zakonodavstvima da reguliraju same sankcije, međutim ukoliko neka članica slučajno i odabere mekšu politiku, Europska komisija zasigurno neće. Stoga je izbor za tvrtke i institucije koje žele nastaviti poslovati u skladu sa zakonom vrlo jednostavan - ili će svoje poslovanje uskladiti sa zahtjevima Uredbe i pratiti praksu vezanu uz primjenu iste kako bi mogli izvršiti reviziju, ukoliko je potrebno, ili će platiti visoku kaznu i nakon naučene lekcije pokrenuti usklađivanje sa zahtjevima Uredbe.

Stoga je glavni motiv za pisanje ovog rada, ujedno i glavni cilj koji se htio istim postići, ukazati na važnost podizanja svijesti o zaštiti posebnih kategorija osobnih podataka, zdravstvenih podataka, te podizanja organizacijskih i tehničkih mjera zaštite osobnih podatka na višu razinu kao i problemi koji proizlaze kroz uspostavu organizacijskih i tehničkih mjera.

2. Zašto Uredba?

Europska direktiva za zaštitu osobnih podataka (engl. General Data Protection Regulation, GDPR) je dokument donesen na razini Europske unije (27. travnja 2016.) koji regulira osnovna načela zaštite osobnih podataka [1].

Dakle, zakonska regulativa koja zahtijeva primjenu ove Uredbe ima svoje uporište kako u međunarodnom tako i u nacionalnom zakonodavstvu i predstavlja zakonsku obavezu, a ne izbor niti smjernicu.

Međunarodno zakonodavstvo

- Konvencija Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podatka (Konvencija 108) i Dodatni protokol uz Konvenciju u vezi nadzornih tijela i međunarodne razmjene podataka
- Direktiva 95/46 EZ o zaštiti osoba s obzirom na postupanje s osobnim podacima te slobodnom protoku takvih podataka
- Uredba (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) – u primjeni od 25. svibnja 2018.
- Povelja o temeljnim pravima Europske unije

Nacionalno zakonodavstvo

- **Ustav** Republike Hrvatske (članak 37.)
- **Zakon** o zaštiti osobnih podataka
- **Uredba** o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka
- **Uredba** o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka

Može se zaključiti kako je ovaj dokument posljedica neujednačene prakse zaštite osobnih podataka u zemljama Europske unije. Zbog te neujednačene prakse europski parlament i europska komisija donijeli su spomenutu Uredbu. Iako je Uredba prilično složen dokument glavne smjernice za primjenu u svakodnevnu praksu predstavljaju njegovih šest načela [1] i to:

- načelo povjerljivosti i cjelovitosti podataka,
- načelo točnosti, potpunosti i ažurnosti u obradi osobnih podataka,
- načelo svrhovitosti obrade osobnih podataka,
- načelo zakonitosti, poštenosti i transparentnosti obrade osobnih podataka,
- načelo odgovornosti (pouzdanosti),
- načelo ograničenosti pohrane.

Kroz sva ta načela provlači se osnovna ideja, a to je:

- sprječavanje narušavanja povjerljivosti i integriteta osobnih podataka,
- sprječavanje neovlaštene dostupnosti podataka te osiguravanje nesmetane i kontinuirane dostupnosti podataka onima koji imaju ovlaštenja.

Što za svakodnevnu praksu u zdravstvenom sustavu znači Uredba?

- regulativa se odnosi na sve one koji upravljaju i obrađuju osobne podatke,
- stoga svaka zdravstvena praksa, javna ili privatna, mora biti u skladu s novim zakonom bez obzira obrađuje li podatke u digitalnom ili papirnatom obliku, ako se Uredba ne primjenjuje u praksi postoji velika vjerojatnost za izricanje novčanih kazni.

2.1 Načela Uredbe

Načela ili pravila ili zakon koji se slijedi, u ovom slučaju principi zaštite osobnih podataka trebala bi se primjenjivati na sve informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Osobne podatke koji su pseudonimizirani, a koji bi se mogli pripisati nekom pojedincu uporabom dodatnih informacija smatraju se informacijama o pojedincu čiji se identitet može utvrditi. Kako bi se odredio identitet pojedinca treba uzeti u obzir sva sredstva koja voditelj obrade ili bilo koja druga osoba mogu po svemu sudeći upotrijebiti u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca. Kako bi se utvrdilo

koja se sredstva za utvrđivanje identiteta pojedinca upotrebljavaju treba uzeti u obzir tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj. Kako bi se dokazalo da je obrada osobnih podataka u skladu s Uredbom ista je upravo definirala šest načela koja obveznicima provedbe Uredbe pomaže u učinkovitom upravljanju ili korištenju ove Uredbe.

2.1.1 Načelo povjerljivosti i cjelovitosti podataka

Osobne podatke trebalo bi obrađivati uz odgovarajuće poštovanje sigurnosti i povjerljivosti osobnih podataka, što obuhvaća i sprečavanje neovlaštenog pristupa osobnim podacima (dodjela autorizacije putem sigurnosnih lozinki, PIN-a, isl.), slučajnog gubitka (hakiranje, računalni virusi itd.), uništenja (npr. uslijed požara) ili oštećenja kao i opremu koja se koristi pri obradi podataka ili njihove neovlaštene upotrebe.

U tom slučaju Uredba je predvidjela ispunjavanje određenih zahtjeva poput:

- Postojanje programa edukacije i podizanja svijesti o potrebi zaštite osobnih podataka.

Vrlo uopćeno taj zahtjev Uredbe podrazumijeva stvaranje klime u organizaciji o potrebi zaštite osobnih podataka. Jedina metoda je konstantna edukacija unutar poslodavca o potrebi zaštite osobnih podataka radi potrebe usklađivanja s Uredbom, ali i zbog očuvanja reputacije same zdravstvene ustanove. Važno je da edukacija bude učinkovita u smislu da svakome bude jasno što mora raditi u vezi s privatnošću (od neposrednog izvršitelja do uprave). Edukacija bi trebala obuhvatiti: osnove Uredbe, informacijsku sigurnost, upravljanje rizicima, definiranje mjera za smanjivanje rizika na prihvatljivu razinu. U velikim zdravstvenim sustavima, poput bolnica, planiranje edukacije predstavlja zahtijevan posao ne samo po pitanju organizacije i provedbe nego i po pitanju kontrole usvojenih znanja iz područja.

- Postojanje upravljanja incidentima

Postoji vjerovanje kako su organizacije koje imaju certifikat za ISO 9001 u prednosti što je jednim dijelom točno jer imaju definiran postupak za rješavanje incidentnih situacija. Ukratko potrebno je definirati procedure kako reagirati ako se incident dogodi. Procedura podrazumijeva vođenje zapisnika o incidentu („Izjava o nesukladnosti“) s naznakom vrste neželjene situacije, kad je nastala, zašto, tko je odgovoran te koja je radnja poduzeta da bi se incident riješio. Vrlo je važno navesti potencijalni ishod – rizik u slučaju kršenja Uredbe. U kontekstu narušene privatnosti, potrebno je razraditi postupak kojim se u roku 72 sata informira osoba o incidentu (o nedostupnosti, neovlaštenom pristupu, narušenom integritetu osobnih podataka, gubitku povjerljivosti osobnih podataka). Dobro je voditi registar incidenata kako bi se uočila eventualna pravilnost incidenata.

Najčešći primjer za ovakvu situaciju je obnavljanje informatičke opreme pri čemu se stara oprema redovito rashoduje i zatim „baca“ bez prethodnog brisanja svih podataka pohranjenih na hardverima osobnih računala. U jednoj zdravstvenoj ustanovi u kojoj se na godišnjoj osnovi obrađuje preko 100.000 osobnih podataka korisnika zdravstvenih usluga kao i osobnih podataka radnika zdravstvene ustanove i te kako predstavlja prijetnju od potencijalne ugroze osobnih podataka.

- Praćenje vanjskih zbivanja.

Kontinuirano praćenje promjena vezanih za zaštitu osobnih podataka je u nadležnosti pravne službe. Ove aktivnosti podrazumijevaju praćenje važećih zakona vezanih uz zaštitu osobnih podataka, rješavanje eventualnih proturječnosti vezanih uz zaštitu osobnih podataka, praćenje stručnih časopisa iz toga područja i slično.

U zdravstvenoj djelatnosti postoji niz raznih zakona i pratećih pravilnika koji u svakodnevnoj praksi reguliraju zakonitost obrade osobnih podataka. Praćenje postojećih zakona i ažuriranih verzija istih izuzetno je bitno u slučaju bilo kakvog odstupanja od uredbe po pitanju zaštite osobnih podataka, a posebno u situacijama podnošenja zahtjeva za pristup osobnim podacima ili upita u koje svrhe se isti obrađuju. Česta je početna zabluda bila ta da se ugovorima između poslodavca i radnika nastoji regulirati tzv. privola kojom radnik daje

dozvolu poslodavcu za obradu njegovih osobnih podataka. Takva aktivnost je posljedica ne poznavanja ostalih zakona koji upravo reguliraju zakonitost poslovanja poslodavca kao i njegu obavezu prema radniku da za potrebe ostvarivanja naknade za ostvareni rad, zdravstveno osiguranje, prijava poreza i sl. postoje niz drugih zakona koji upravo reguliraju ovakve obaveze poslodavca.

- Postojanje strukture upravljanja osobnim podacima

Ukoliko se želi uspješno uskladiti s Uredbom, treba shvatiti da u tome treba sudjelovati cijela organizacija. Treba definirati odgovornost za zaštitu osobnih podataka, od uprave do neposrednih izvršitelja. Uloge u zaštiti osobnih podataka treba definirati internim pravilnikom o zaštiti osobnih podataka, njegovom javnom objavom kao garancija svima, radnicima i korisnicima usluga, da se ne narušava privatnost osobnih podataka pacijenata ako je u kontaktu s tim podacima. Ovdje treba definirati način komunikacije s nacionalnim regulatorom (AZOP), kako ga izvješćivati o zaštiti osobnih podataka u organizaciji. Najčešće se lome koplja oko uloge i pozicije službenika za zaštitu osobnih podataka. Ovaj pojedinac koji je imenovan od Uprave za obavljanje savjetodavnih i operativnih zadataka u skladu sa zahtjevima Uredbe mora bit dio Uprave i dio svih bitnih upravljačkih tijela unutar poslodavca.

- Postojanje upravljanja informacijskom sigurnošću.

Potrebno je definirati način kako osigurati povjerljivost osobnih podataka, njihov integritet (zabranu neovlaštene promjene) te dostupnost podataka onima koji na to imaju pravo. Standard o informacijskoj sigurnosti, posebno standard ISO 27799 koji se bavi upravljanjem informacijske sigurnosti u zdravstvu daje jako dobre smjernice po pitanju zaštite podataka koje se temelje na kvalitetnom upravljanju rizicima (što je bit upravljanja informacijskom sigurnošću). Cilj toga zahtjeva Uredbe jest tzv. PIA (engl. Personal Impact Analysis) tj. upravljanje rizicima [9].

Naglasak pri upravljanju rizicima jest na ranjivosti sustava vezano uz osobne podatke, vjerojatnosti da sigurnosne prijetnje iskoriste postojeću ranjivost te da nastane rizik kao funkcija ranjivosti sustava i vjerojatnosti pojave prijetnje. Bitno je prepoznati koji su to rizici te ih opisati. Mogući koraci prilikom izrade procjene rizika po pitanju zaštite osobnih podataka su sljedeći:

Opseg rizika	**Definiranje rizika**	**Strane koje na direktan ili indirektan način sudjeluju u riziku**	**Kvalifikacija rizika**
kvalitativan opis događaja, veličine, tipa, broja i ovisnosti	strateški, operativni, financijski, znanje	tko je zainteresiran za upravljanje i njihova očekivanja	važnost i vjerojatnost nastanka
Tolerancija rizika	**Odnos prema riziku i kontrolni mehanizmi**	**Strategija i razvoj politike**	
potencijalni gubitak i financijska šteta, željene kontrole i razina izvedbe	razine pouzdanosti postojećih kontrola, identifikacija protokola za nadzor i izvještavanje	identifikacija funkcija odgovornih za razvoj strategija i politike	

Nakon prvog odrađenog koraka potrebno je ustrojiti i voditi registar rizika vezanih uz osobne podatke. Registar rizika zahtjeva definiranje organizacijskih, fizičkih i logičkih kontrola koje bi rizike vezane uz osobne podatke trebale smanjiti na prihvatljivu razinu. U zdravstvenoj djelatnosti treba voditi registar rizika za svaku specifičnu djelatnost posebno. Ovdje treba uključiti stručnjake za svako područje.

Dakle potrebno je:

- navesti naziv ustrojstvene organizaciju u kojoj postoji potencijalni rizik,
- navesti točan naziv rizika u ovoj ustrojstvenoj organizaciji,
- navesti točan naziv svih kontrolnih mehanizama za svaki rizik zasebno
  - politika privatnosti ili izjave zaposlenika da će štititi privatnost podataka;
  - čuvanje papirnate arhive u posebnoj prostoriji pod ključem ili zaključavanje sistemske sobe sa serverima;
  - logička kontrola je korisničko ime i zaporka korisnika informacijskih sustava.
- procijeniti svaki rizik s obzirom na vjerojatnost pojavljivanja i potencijalnu štetu koju može izazvati,

- u slučaju nastanka štete definirati procedure upravljanja incidentnim situacijama, postavit rokove za uklanjanje štete i odgovorne osobe za upravljanje rizicima i provedbu popravnih radnji.

Zahtjev usklađenosti i pouzdanosti nemoguće je ispuniti bez propisane politike koja mora biti u pisanom obliku. Bez obzira zove li se taj pisani dokument politika, pravilnik, odluka i sl., politika zaštite osobnih podataka je dokaz da je organizacija sustavno provela zaštitu osobnih podataka. Struktura politike zaštite podataka ovisi o vrsti obveznika, vrsti i kategorijama podataka koje obrađuje, a osobito o načinima i procesima obrade. Obveznici provedbe Opće uredbe, posebno u zdravstvenoj djelatnosti, iako obrađuju manje-više iste kategorije i vrste osobnih podataka, to nikako ne znači da su svrha, načini i procesi obrade isti.

Politikom zaštite osobnih podataka obveznik treba utvrditi svoje specifične svrhe, načine, postupke, organizaciju obrade i osobito tehničke i organizacijske mjere zaštite kako bi dokazali da je zahtjev Opće uredbe po pitanju usklađenosti i pouzdanosti ispunjen.

Jednom utvrđeni načini i tehnologije obrade osobnih podatka u Politici moraju stvarno egzistirati u svakodnevnoj praksi kod obveznika. Isto vrijedi i za utvrđivanje svih kategorija i vrsta osobnih podataka i načinu njihove obrade.

Cjelovita politika u svojem normativnom dijelu treba sadržavati uređenje najmanje sljedećih pitanja [10]:

- opću politiku zaštite osobnih podataka i temeljna načela
- sustav pohrane osobnih podataka (kategorije ispitanika, osnove, svrhu i način obrade, vlasnike osobnih podataka, osobe koje obrađuju osobne podatke)
- organizaciju, upravljanje i nadzor
- ovlasti i odgovornosti organizacijskih dijelova i osoba
- imenovanje, ovlasti i odgovornosti službenika za zaštitu podataka (ako se imenuje)
- tehničke i organizacijske mjere zaštite osobnih podataka (primjenu načela privatnosti po dizajnu i po zadanim postavkama, tehničke mjere zaštite, informatičke mjere zaštite, organizacijske mjere zaštite)
- odnos s izvršiteljem obrade
- način provedbe procjene rizika i procjene učinka na zaštitu podataka
- prijenos osobnih podataka trećim stranama
- uvjete i način pribavljanja i uskraćivanja privola ispitanika
- informiranje ispitanika
- ostvarivanje prava ispitanika
- postupke odgovora na povrede osobnih podataka i izvješćivanje
- evidenciju aktivnosti obrade
- rokove čuvanja osobnih podataka i način brisanja.

Treba naglasiti da pacijenti trebaju imati pravo na promjenu podataka, pravo na zaborav. Također, politika treba naglasiti etičnost u obradi osobnih podataka [11].

- Upravljanje rizicima trećih strana.

Potrebno je definirati odnos s partnerima (npr. HZZO, HZJZ, dobavljači). Imaju li podaci koji se razmjenjuju narav osobnih podataka? Može li do tih podataka neovlašteno doći netko nepoželjan? Razmjenjuju li se podaci u kriptiranom obliku ili ne? Od dobavljača programa i informacijskih sustava potrebno je zatražiti da implementiraju svoja rješenja u zaštitu osobnih podataka te prilikom potpisivanja ugovora ugraditi klauzulu kojom se obvezuju da štite osobne podatke pacijenata i radnika.

- Postojanje nadzora nad provođenjem operativnih postupaka.

Uredba zahtjeva da se prilikom uvođenja novih informacijskih sustava vodi računa o zaštiti osobnih podataka. Pri uvođenju novih funkcionalnosti, potrebno je procijeniti štite li se u dovoljnoj mjeri osobni podatci. Kod novih verzija programa treba identificirati rizike vezane uz osobne podatke, treba definirati zaštitne mehanizme i tražiti dobavljače softvera da te mehanizme implementiraju.

- Nadzor nad postupcima rukovanja osobnim podacima.

Potrebno je stalno provjeravati primjenu procedure zaštite osobnih podataka putem internih audita. Procedure je potrebno ažurirati u slučaju incidenata (nedostupnosti, narušavanja povjerljivosti i integriteta – „curenje“ podataka ili neovlaštena promjena podataka). Potrebno je imati zapise o provjeri sustava zaštite privatnosti podataka. Spomenuto je potrebno osigurati kako bi se mogla dokazati sukladnost s Uredbom u slučaju kontrole nadležnih institucija.
Ispunjavanje svih tih zahtjeva osigurava integraciju zaštite osobnih podataka u poslovanje. Nasuprot tome, neispunjavanje tih zahtjeva znači izlaganje riziku za neusklađenost s Uredbom. Da bi se ispunila načela te zahtjevi Uredbe, zdravstvene organizacije moraju se prilagoditi Uredbi.

2.1.2 Načelo točnosti, potpunosti i ažurnosti u obradi osobnih podataka

Trebalo bi poduzeti svaki razumno opravdani korak radi osiguravanja da se netočni osobni podaci isprave ili izbrišu. U zdravstvenom sustav primjeri koji upućuju na važnost poštivanja ovog načela vide se u nekim od sljedećih aktivnosti:

- interdisciplinarna suradnja raznih odjela i službi,
- upravljanje i slanje elektroničkih računa i izvješća HZZO-u,
- portal zdravstva,
- upravljanje i slanje elektroničkih izvješća HZJZ-u,
- planiranje poslovanja zdravstvene ustanove itd.

2.1.3 Načelo svrhovitosti obrade osobnih podataka

Osobni podaci trebali bi se obrađivati samo ako za to postoji opravdana svrha: posebna, izričita ili zakonska. Ili ukoliko se obrada osobnih podataka ne bi mogla opravdano postići drugim sredstvima. Jedan od tih načina je i privola ili neka druga legitimna osnova.

Međutim, kako bi obrada bila zakonita**,** navedeni oblici obrade osobnih podataka moraju biti propisani ovom Uredbom bilo u drugom pravu Unije ili pravu države članice na koji upućuje ova Uredba, uključujući obvezu poštovanja pravne obveze kojoj podliježe voditelj obrade ili obvezno izvršavanje ugovora u kojem je ispitanik jedna od stranaka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora.

Ukoliko obrada osobnih podataka nije u skladu s navedenom svrhom ista se morao obustaviti. Jedan od takvih primjera je fotografiranje pacijenta za potrebe javne objave. U ovakvim slučajevima obaveza je onoga koji želi objaviti fotografije pacijenta od njega ili njegovog zakonskog skrbnika zatražiti dozvolu putem privole s točnom definiranom svrhom objave, datum traženja pristanka na privolu, rokom do kada privola vrijedi s mogućnošću povlačenja privole onda kada pacijent to odluči.

2.1.4 Načelo zakonitosti, poštenosti i transparentnosti obrade osobnih podataka

Svaka obrada osobnih podataka trebala bi biti zakonita i poštena. Za pojedince bi trebalo biti transparentno kako se osobni podaci koji se odnose na njih prikupljaju, upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti osobni podaci obrađuju ili će se obrađivati.

- Zakonitost obrade osobnih podataka

Obrada bi se trebala smatrati zakonitom ako je potrebna u kontekstu ugovora ili namjere sklapanja ugovora.

Ako se obrada odvija u skladu s pravnim obvezama kojima podliježe voditelj obrade ili ako je obrada potrebna za izvršavanje zadaće koja se obavlja u javnom interesu ili pri izvršavanju službene ovlasti, obrada bi se trebala temeljiti na pravu Unije ili pravu države članice.

Ovom se Uredbom ne zahtijeva potreba posebnog propisa za svaku pojedinačnu obradu. Jedan propis kao osnova za više postupaka obrade, koji se temelje na pravnoj obvezi kojoj podliježe voditelj obrade ili ako je obrada potrebna za izvršenje zadaće koja se provodi zbog javnog interesa ili pri izvršavanju službene ovlasti, može biti dovoljan.

Uredba uređuje zakonitost obrade osobnih podataka, utvrđuje specifikacije za utvrđivanje voditelja obrade, vrste osobnih podataka koji podliježu obradi, dotičnih ispitanika, subjekata kojima se osobni podaci mogu otkriti, ograničenja svrhe, razdoblja pohrane i drugih mjera za osiguravanje zakonite i poštene obrade. Bez obzira je li voditelj obrade obavlja zadaću u javnom interesu ili prilikom izvršavanja službene ovlasti te je li nastupa kao tijelo javne vlasti ili druga fizička ili pravna osoba koja posluje sukladno javnom pravu ili privatnom pravu, obrada osobnih podataka je opravdana i od javnog interesa u slučaju javnog zdravlja i socijalne zaštite te upravljanja službama za zdravstvenu skrb.

- Načelo poštenosti

Ovo načelo ne ide bez transparentnosti obrade koje zahtjeva da ispitanik bude informiran o postupku obrade i njegovim svrhama. Voditelj obrade trebao bi ispitaniku pružiti sve dodatne informacije neophodne za osiguravanje poštene i transparentne obrade uzimajući u obzir posebne okolnosti i kontekst obrade osobnih podataka.

- Načelo transparentnosti

Traži se da svaka informacija i komunikacija u vezi s obradom tih osobnih podataka bude lako dostupna i razumljiva te da se upotrebljava jasan i jednostavan jezik. To se načelo osobito odnosi na informacije ispitaniku o identitetu voditelja obrade i svrhama obrade te daljnje informacije radi osiguravanja poštenosti i transparentnosti obrade s obzirom na pojedince o kojima je riječ i njihovo pravo da dobiju potvrdu i na obavijest o osobnim podacima koji se obrađuju, a koji se odnose na njih. Pojedinci bi trebali biti upoznati s rizicima, pravilima,

zaštitnim mjerama i pravima u vezi s obradom osobnih podataka i načinom ostvarenja svojih prava u vezi s obradom. Osobito, određena svrha u koju se osobni podaci obrađuju trebala bi biti izrijekom navedena i opravdana te određena u vrijeme prikupljanja osobnih podataka. Osobni podaci trebali bi biti primjereni, bitni i ograničeni na ono što je nužno za svrhe u koje se podaci obrađuju. Zbog toga je osobito potrebno osigurati da je razdoblje u kojem se osobni podaci pohranjuju ograničeno na strogi minimum.

Načelom transparentnosti zahtjeva se da svaka informacija namijenjena javnosti ili ispitaniku bude sažeta, lako dostupna i razumljiva, da se upotrebljava jasan i jednostavan jezik. Takva bi se informacija također mogla dati u elektroničkom obliku, na primjer na internetskim stranicama, kada je namijenjena javnosti. To je osobito bitno u situacijama u kojima zbog velikog broja sudionika i tehnološke složenosti prakse ispitaniku nije lako prepoznati i razumjeti prikupljaju li se osobni podaci o njemu, tko ih prikuplja i u koju svrhu.

Propisi nalažu da poslodavac, npr. zdravstvena ustanova, mora informirati pacijente o tome što se radi s njihovim osobnim podacima. U tu svrhu poslodavac izrađuje Politiku o zaštiti osobnih podataka i privatnosti i javno je objavljuje na web stranicama [12].

U ovo načelu Uredba predviđa ispunjavanje još jednog zahtjeva, a to je osiguranje pojedincu za podnošenje zahtjeva na prigovor po pitanju zaštite osobnih podataka.

- Postojanje upravljanja zahtjevima i prigovorima

Uredba je u ovom slučaju vrlo jasna. Trebalo bi predvidjeti modalitete kojima se olakšava ostvarivanje prava ispitanika iz ove Uredbe, uključujući mehanizme za podnošenje zahtjeva te ako je primjenjivo, besplatno ostvarivanje, osobito zahtjeva za pristup osobnim podacima, njihovo ispravljanje ili brisanje i ostvarivanje prava na prigovor. Voditelj obrade trebao bi također pružiti sredstva za elektroničku predaju zahtjeva, osobito ako se osobni podaci obrađuju elektronički. Voditelj obrade trebao bi biti dužan odgovoriti na zahtjev ispitanika bez nepotrebnog odgađanja i najkasnije u roku od mjesec dana te iznijeti razloge ako voditelj obrade nema namjeru ispuniti bilo koji takav zahtjev. Dakle, Uredba zahtjeva vođenje evidencije prigovora osoba za koje postoje osobni podatci (zaposlenici, bolesnici, partneri). Potrebno je definirati proceduru podnošenja pritužbi vezanih uz narušavanje dostupnosti, povjerljivosti i integriteta osobnih podataka. Mora biti jasno kako i kome se žaliti. Potrebno je pratiti razloge

pritužbi. Isto tako, osim pritužbi mora se uspostaviti mehanizam kako se zahtjeva pristup osobnim podacima, kako se osobni podaci ažuriraju, brišu, kako se podaci izvoze i daju korisniku.

2.1.5 Načelo odgovornosti

Ovo načelo može se najjednostavnije objasniti kao sposobnost dokazivanja da je obrada osobnih podataka u skladu sa svim načelima Opće uredbe o zaštiti osobnih podataka.

Najjednostavniji način kako to utvrditi je preko kontrole ispunjavanja zahtjeva Uredbe. Potrebno je analizirati svaki od zahtjeva i provjeriti je li zahtjev ispunjen, u kojoj je mjeri ispunjen, što još treba napraviti. Osim toga treba razmisliti o odgovorima na sljedeća pitanja [13]:

- Koje se informacije prikupljaju?
  - podaci o zaposlenicima,
  - podaci o korisnicima zdravstvene zaštite,
  - podaci o poslovnim partnerima,
- Tko ih prikuplja?
  - kadrovska služba,
  - svi djelatnici koji na direktan ili indirektan način sudjeluju u procesu liječenja,
  - odjel nabave,
- Kako se prikupljaju?
  - prilikom zapošljavanja, prilikom promjene kvalifikacija u svrhe obračuna plaće,
  - dolaskom pacijenta na odjel,
  - prilikom raspisivanja tendera o nabavi,
- Zašto se prikupljaju?
  - evidencija zaposlenika radi ostvarenja materijalnih prava,
  - u medicinske svrhe,
  - zbog sklapanja potencijalnih poslovnih odnosa,
- Kako se koriste?
  - poslovni informacijski sustavi,

    - aplikacije o plaćama,
    - aplikacije za fakturiranje,
    - aplikacije prijave i odjave radnika,
- S kime će se podijeliti?
    - odjel ljudskih resursa,
    - odjel za obračun plaća,
    - sva radilišta poliklinike – CEZIH,
    - odjel nabave – skladištenje – poslovni informacijski sustav – registar ugovora,
    - odjel za fakturiranje,
    - blagajne,
    - prijemni šalteri,
- Koji je učinak na pojedince na koje se prikupljanje informacija odnosi?
- itd.…

Kao što se može primijetiti svako ovo pitanje automatski traži definiranje svrhe i jedne od zakonske osnove na temelju koje se vrši obrada osobnih podataka.
Odgovori na ta pitanja mogu pomoći zdravstvenim djelatnicima pri usklađivanju poslovanja s Uredbom, a mogu pomoći i smjernice o tome što napraviti da bi se ispunio svaki od zahtjeva Uredbe [1], [14].

Zato je Uredba ustrojila još jedna zahtjev, a to je vođenje registra osobnih podataka, koji predstavlja tzv. zbirku osobnih podataka koja daje na uvid gdje se sve prikupljaju osobni podaci, tko ih prikuplja, zašto ih prikuplja i kada.

Takav registar pomaže organizaciji da u svakome trenutku zna s kojim osobnim podacima rukuje. Registar treba redovito provjeravati i održavati.

Ovo načelo također podrazumijeva primjenu tehničkih i organizacijskih mjera u pogledu ograničavanja obrade osobnih podataka koje uključuju privremeno premještanje odabranih osobnih podataka u drugi sustav obrade, činjenje odabranih podataka nedostupnima za korisnike ili privremeno uklanjanje objavljenih podataka s internetske stranice. U automatiziranim sustavima pohrane ograničavanje obrade u načelu bi trebalo osigurati tehničkim sredstvima na način da osobni podaci nisu predmet daljnjih obrada i da se ne mogu

mijenjati. Činjenicu da je obrada osobnih podataka ograničena trebalo bi jasno navesti u sustavu.

Radi dodatnog jačanja nadzora nad vlastitim podacima, kada se obrada obavlja automatskim putem, ispitaniku bi se također trebalo dopustiti da osobne podatke koji se odnose na njega, a koje je dao voditelju obrade dobije u strukturiranom, uobičajeno upotrebljavanom, strojno čitljivom i interoperabilnom formatu i da ih prenese drugom voditelju obrade. Voditelje obrade trebalo bi poticati na razvijanje interoperabilnih formata koji omogućuju prenosivost podataka. To bi se pravo trebalo primjenjivati u slučajevima kad je ispitanik osobne podatke dao na temelju svoje privole ili kad je obrada nužna za izvršenje ugovora. To se pravo ne bi smjelo primjenjivati ako se obrada temelji na drugoj pravnoj osnovi koja nije privola ili ugovor. Samom svojom prirodom to se pravo ne može ostvariti u slučaju da voditelji obrade osobne podatke obrađuju u okviru svojih javnih dužnosti. Stoga se ono ne bi smjelo primjenjivati ako je obrada osobnih podataka nužna kako bi se poštovala pravna obveza kojoj voditelj obrade podliježe ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade.

Pravo ispitanika na prijenos ili primanje osobnih podataka koji se odnose na njega ne bi trebalo obvezivati voditelja obrade da upotrebljava ili održava tehnički kompatibilne sustave za obradu. Ako se određeni skup osobnih podataka odnosi na više ispitanika, pravo na primanje tih osobnih podataka ne bi smjelo dovoditi u pitanje prava i sloboda ostalih ispitanika u skladu s ovom Uredbom. Nadalje, tim pravom također se ne bi smjelo dovoditi u pitanje pravo ispitanika na brisanje osobnih podataka, kao i ograničenja tog prava, kako je navedeno u ovoj Uredbi, te ono osobito ne bi smjelo podrazumijevati brisanje osobnih podataka koji se odnose na ispitanika, koje je on dostavio u svrhu izvršavanja ugovora, u mjeri u kojoj su ti osobni podaci potrebni za izvršavanje tog ugovora i koliko god su potrebni. Ako je tehnički izvedivo, ispitanik bi trebao imati pravo na to se osobni podaci prenose izravno između voditelja obrade.

Dakle, voditelj obrade trebao bi poduzeti odgovarajuće tehničke i organizacijske mjere kako bi se posebno osiguralo da budu ispravljeni čimbenici koji dovode do netočnosti u osobnim podacima i da se rizici od pojave pogrešaka svedu na minimum, te osobne podatke osigurati na način kojim se uzima u obzir potencijalne rizike za interese i prava ispitanika i kojim se, među ostalim, sprečavaju diskriminacijski učinci na pojedince na temelju rasnog ili

etničkog porijekla, političkog mišljenja, vjere ili uvjerenja, članstva u sindikatu, genetskog ili zdravstvenog stanja ili spolne orijentacije, ili koji rezultiraju mjerama koje imaju takav učinak.

2.1.6 Načelo ograničenosti pohrane

Radi osiguravanja da se osobni podaci ne drže duže nego što je nužno, voditelj obrade trebao bi odrediti rok za brisanje ili periodično preispitivanje. Čuvati u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Osobni podaci mogu se pohraniti na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja i to u javne svrhe kao i u svrhe znanstvenog istraživanja i sl.

Ovo načelo obuhvaća i još jedan zahtjev, a on se odnosi na upravljanje privolama i izjavama o privatnosti.

- Postojanje privola (pristanaka) i izjava o privatnosti

Ovaj zahtjev podrazumijeva osiguranje pisanog pristanak svih osoba o kojima se prikupljaju podaci (iz registra osobnih podataka) za prikupljanje podataka i to kada svrha obrade osobnih podataka nije uvjet za ostvarenje neke od usluga i kada nema uporište u zakonu. Zakonom o podacima i informacijama u zdravstvu [15] zahtjeva se od svih radnika koji na direktan ili indirektan način sudjeluju u procesu liječenja pisana izjava privatnosti kojom se obvezuju na tajnost povezanu uz osobne podatke, u kojoj je definirana odgovornost radnika ukoliko prekrše izjavu o privatnosti. Što se tiče bolesnika kod njih je eksplicitna privola potrebna samo u slučaju da se podaci o bolesnicima želi iskoristiti u svrhu nekih statističkih obradba, znanstvenih istraživanja ili ispitivanja novih načina liječenja. U slučaju pružanja medicinske skrbi, ne smije se tražiti privola jer pružanje medicinske skrbi regulirano je mnogobrojnim zakonima. U slučaju nekih rizičnih dijagnostičko-terapijskih postupaka, obaveze je potpisivanje Izjave o informiranom pristanku/odbijanju predloženog dijagnostičko terapijskog postupka, a kojeg bolesnik potpisuje na osnovi dobivenih informacija od liječnika. Međutim, ova Izjava je regulirana Zakon o pravima pacijenata [16] i ne smije se nikad zamijeniti privolom.

3. Definiranje najvažnijih pojmova Uredbe

Uredba o zaštiti osobnih podataka na samom svom početku sastoji se od niza pojmova koje detaljno objašnjava. Međutim, ono što je za svakodnevnog zdravstvenog ali i nezdravstvenog praktičara bitno, je izdvojiti i razumjeti najvažnije pojmove onih sudionika u svakodnevnom procesu izmjene osobnih podataka. Ovdje će se posebno izdvojiti neki od njih poput: osobni podatak, obveznici primjene Uredbe kao poslovni subjekti s obzirom na njihove uloge: voditelj obrade, izvršitelj obrade, ispitanik, privola, obrada osobnih podataka.

3.1 Osobni podaci

Osobni podaci su podaci koji su po svojoj naravi posebno osjetljive prirode u pogledu temeljnih prava i sloboda te kao takvi zaslužuju posebnu zaštitu jer bi u okviru njihove obrade moglo doći do značajnih rizika za temeljna prava i slobode. Koliko su osobni podaci osjetljivi može se objasniti kroz vezu raznih mehanizama kojima se obrađuju isti [17].

Osobni podaci

Definicija	Načela obrade osobnih podataka	Osnova za obradu	Gdje se sve skrivaju
• skup podataka koji omogućava identificiranje pojedinca: • ime i prezime, adresa, OIB, bankovni računi, informacije o lokaciji, fotografija, genetički i biometrijski podaci, postovi na društvenim mrežama, medicinske informacije, IP adrese i web-kolačići	• zakonitost, poštenje, transparentnost, ograničavanje svrhe, ograničavanje količine podataka, točnost, ograničavanje pohrane, cjelovitost i povjerljivost, pouzdanost	• zakonska obaveza • ugovorna obaveza • privola	• kadrovska služba, • pravna služba, • jedinice za operativno poslovanje, • financijska služba, • prodaja i marketing, • IT služba, • vanjski partneri

Posebne kategorije osobnih podataka, u zdravstvenoj djelatnosti na prvom mjestu su to svi medicinski podaci, zaslužuju veći stupanj zaštite i trebaju se obrađivati samo u svrhe povezane sa zdravljem radi ostvarivanja tih svrhâ u korist pojedinaca i društva u cjelini. Ovo se posebno odnosi na kontekst upravljanja uslugama i sustavima zdravstvene ili socijalne skrbi.

Tu se ubraja obrada ovakvih podataka i to u svrhu kontrole kvalitete, informacija o upravljanju i općeg nacionalnog i lokalnog nadzora sustava zdravstvene ili socijalne skrbi. Kada obradu posebnih kategorija osobnih podataka provodi uprava i središnja nacionalna tijela nadležna za zdravlje njihova svrha obrade posebnih kategorija osobnih podataka je u svrhu osiguravanja kontinuiteta zdravstvene ili socijalne skrbi i prekogranične zdravstvene skrbi ili u svrhe zdravstvene zaštite, nadzora i uzbunjivanja, ili u svrhe arhiviranja u javnom interesu, u svrhe znanstvenih ili povijesnih istraživanja ili u statističke svrhe. Svaka svrha obrade posebnih kategorija osobnih podataka mora biti utemeljena na pravu Unije ili pravu države članice jer se na temelju tog prava definiraju ciljevi obrade ove kategorija osobnih podataka koji su najčešće od javnog interesa, kao i za studije koje se provode u javnom interesu u području javnog zdravlja. Primjerice obrada osobnih podataka pojedinaca zaraženih COVID-om-19, ili preventivno prikupljanje podataka svih korisnika zdravstvene zaštite u prostoru trijaže zdravstvene ustanove.

Uredba utvrđuje uvjete za obradu posebnih kategorija osobnih podataka koji se odnose na zdravlje, za posebne potrebe, osobito kada obradu takvih podataka za određene zdravstvene svrhe provode osobe koje podliježu zakonskoj obvezi čuvanja poslovne tajne. Pravom Unije ili pravom države članice trebalo bi predvidjeti specifične i primjerene mjere za zaštitu temeljnih prava i osobnih podataka pojedinaca. Državama članicama trebalo bi omogućiti zadržavanje ili uvođenje dodatnih uvjeta, uključujući ograničenja, u vezi s obradom genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje. Međutim, to ne bi trebalo spriječiti slobodan protok osobnih podataka unutar Unije ako se ti uvjeti primjenjuju na prekograničnu obradu takvih podataka.

Obrada posebnih kategorija osobnih podataka bez privole ispitanika može biti potrebna zbog javnog interesa u područjima javnog zdravlja. Takva bi obrada trebala podlijegati primjerenim i specifičnim mjerama kako bi se zaštitila prava i slobode pojedinaca. U tom bi kontekstu „javno zdravlje" trebalo tumačiti kako je definirano u Uredbi (EZ) br. 1338/2008 Europskog parlamenta i Vijeća [6], što znači *svi elementi povezani sa zdravljem, tj. zdravstvenim stanjem,* uključujući morbiditet i invaliditet, determinante koje utječu na to zdravstveno stanje, potrebe zdravstvene zaštite, sredstva dodijeljena zdravstvenoj zaštiti, pružanje zdravstvene zaštite i opća dostupnost zdravstvene zaštite, kao i troškovi i financiranje zdravstvene zaštite te uzroci smrtnosti. Takva obrada podataka koja se odnosi na zdravlje za

potrebe javnog interesa ne bi smjela prouzročiti obradu osobnih podataka u druge svrhe koju obavljaju treće strane kao što su poslodavci ili osiguravajuća društva.

3.2 Obveznici provedbe Uredbe - Poslovni subjekti

Ovdje je bitno definirati uloge poslovnih subjekta s obzirom na specifične uloge i odgovornosti koji svaki od njih posjeduje [17].

Poslovni subjekti

Voditelj obrade	**Zajednički voditelj obrade**	**Izvršitelj obrade**	**Primatelj**

U središtu njihove djelatnosti je ispitanik

Najčešći problem nastaje kod određivanja funkcije voditelja i izvršitelja obrade. Važnost točnog definiranja uloge onoga koji obrađuje osobne podatke nalazi se u činjenici što za različite vrste poslovnih subjekata proizlaze donekle različite obveze iz Uredbe. Isto tako potrebno je odrediti uloge drugih subjekata koji provode određene radnje obrade zajedno s obveznikom ili nakon njega. Sukladno uredbi navest će se nekoliko definicija najvažnijih pojmova Uredbe [17].

Voditelj obrade

Definicija	Obrada osobnih podataka	Propisi	
Fizička ili pravna osoba koja sama određuje svrhu i sredstva obrade ili je to određeno propisom.	Temelji se na nekom propisu, Ako obradu osobnih podataka ne određuje propis (propis RH ili EU), tada obradu određuje sam voditelj obrade, s tim što odlučuje da će provoditi neke od postupaka obrade određenih kategorija osobnih podataka	Zakoni i pripadajući podzakonski akti: uređuju tko je dužan provoditi obradu osobnih podataka, koju vrstu osobnih podataka, koliko dugo (rokove čuvanja), kome ih mora dostavljati	• Zakon o radu(NN 93/14 i 127/17) • Zakoni kojima se uređuju porezi i obvezni doprinosi • Zakon o zaštiti na radu • Zakon o obveznom zdravstvenom osiguranju itd.

Dakle, v**oditelj obrade,** tj. poslodavac je pravni subjekt koji temeljem važećih propisa i podzakonskih akata mora prikupljati, obrađivati i prenositi osobne podatke o svim ispitanicima (radnici, pacijenti, klijenti itd.) s kojima je u poslovnom odnosu.

Pored već postojećeg voditelja obrade može postojati i više voditelja iste obrade, tada su oni **zajednički voditelji obrade** (npr. poslodavac čija je osnovna djelatnost zdravstvo, HZZO, FINA itd.). Zajednički voditelji obrade su oni koji zajednički određuju svrhu obrade ili su takvima određeni propisom. Tu je okolnost važno utvrditi jer to utječe na upravljanje postupcima obrade te nadzor nad obradom, ali iz te okolnosti proizlazi i zajednička odgovornost za postupke obrade.

Unutar grupe obveznika koji zajednički djeluju (npr. grupa povezanih društava), često se obavljaju pojedine radnje obrade osobnih podataka za neke zajedničke potrebe ili zajedničkim resursima, primjerice zajedničkim aplikacijama ili na zajedničkom poslužitelju. U takvim slučajevima potrebno je pažljivo definirati uloge, da bi se razgraničile obveze i odgovornosti.

Izvršitelj obrade

Definicija	**Aktivnost obrade**	Može obavljati jednu ili više radnji obrade	
Fizička ili pravna osoba koja obradu obavlja u ime voditelja obrade (čl. 4. točka 8. Opće uredbe) temeljem ugovora.	Po nalogu voditelja obrade i u njegovo ime obrađuje osobne podatke ispitanika voditelja obrade.	Prikuplja i pohranjuje osobne podatke	Prikuplja, koristi, prenosi i pohranjuje osobne podatke drugim poslovnim subjektima

Sljedeći podaci trebali bi voditeljima obrade pomoći pri definiranju uloga i odgovornosti na relaciji voditelj – izvršitelj obrade s obzirom na sljedeće kriterije [17].

Kriterij	**Voditelj obrade**	**Izvršitelj obrade**
-tko određuje svrhu obrade	-određuje svrhu obrade ili je određena propisom	-ne određuje svrhu obrade
-za koga se provodi obrada	-provodi obradu u svoje ime	--provodi obradu u ime voditelja obrade, po njegovom nalogu
-samostalnost obrade	-samostalno obrađuje osobne podatke	-nesamostalan je, ovisan je voditelju obrade

Dakle, **izvršitelj obrade** je samo onaj kome je voditelj obrade dao izričitu ovlast da u njegovo ime izvršava određene radnje obrade osobnih podataka njegovih ispitanika i to tako što je voditelj obrade izvršitelju obrade točno odredio koji će se osobni podatci prikupljati, obrađivati, pohranjivati i dr.

Na primjer, svaki od obveznika jest voditelj obrade za sebe, međutim, s obzirom na djelatnost koju obavlja može imati funkciju i izvršitelja obrade. Ovdje se mogu svrstati knjigovodstveni servisi, sami za sebe su voditelji obrade, ali za svoje klijente oni su izvršitelji obrade. No, moguće je da i knjigovodstveni servis koristi određene usluge nekog trećeg u obradi, pa će i sam imati izvršitelja obrade.

Primatelji osobnih podataka treće su osobe kojima se prenose osobni podaci bilo da je to određeno propisom bilo da je to odredio voditelj obrade. Primatelji osobnih podataka i drugi su voditelji obrade i izvršitelji obrade kojima voditelj obrade prenosi osobne podatke radi izvršenja njihove obrade odnosno obrade u ime voditelja obrade. Dakle, primatelji osobnih podataka mogu biti izvršitelji obrade za voditelja obrade koji im je prenio podatke, ali i ne moraju to biti. U ovome drugom slučaju sam će primatelj osobnog podatka u svojim postupcima obrade tih osobnih podataka biti u ulozi voditelja obrade.

Po pitanju uloga naručitelja određene IT usluge i izvršitelja takve usluge treba biti oprezan pri ugovaranju takvih usluga i određivanja uloga u obradi osobnih podataka. Ako je IT izvršitelj isporučitelj neke aplikacije kojom se obrađuju osobni podaci te pruža uslugu održavanja takve aplikacije (ažuriranje, nadogradnja, otklanjanje pogrešaka), on u tome ne obavlja radnje obrade osobnih podataka pa nije izvršitelj obrade za naručitelja. No, ipak, ako je opseg usluge proširen i na pohranu podataka kod IT isporučitelja, njegov unos osobnih podataka, ispravke ili druge radnje na osobnim podacima, tada će IT isporučitelj imati ulogu izvršitelja obrade. Usluga samog spremanja osobnih podataka također predstavlja radnju obrade osobnih podataka, pa ako takvu uslugu pruža IT isporučitelj, on je izvršitelj obrade [10]

Definiranje uloga i odgovornosti voditelja i izvršitelja jako je važno posebno u procesu analize rizika. Primjera radi u zdravstvenoj djelatnosti mogu se koristiti sofisticirani uređaji u dijagnostičke svrhe koji osim RTG snimanja pohranjuju i osobne podatke svakog pojedinog pacijenta uz određeni snimak. Poput: imena i prezimena, broj zdravstvenog osiguranja, količinu primljene doze zračenja, broj izlaganja ionizirajućem zračenju itd. Problem nastaje u trenutku

nastanka „kvara“ na takvim uređajima – ne u pogledu ispravnosti po pitanju ionizirajućeg zračenja već po pitanju ispravnosti rada softvera koji pohranjuje sve navedene podatke svaki put kada je pacijent sniman. U tom trenutku zdravstvena ustanova ima potrebu za određenom uslugom od ovlaštenog tehničkog servisa kako bi se isti softver popravio, ali u ovom slučaju tehnički servis ne nastupa samo kao serviser opreme nego i kao izvršitelj obrade jer mu se treba dozvoliti pristup osobnim podacima i osigurati njihovo backupiranje. U ovom trenutku nastaje problem jer tehnički servisi ne žele na sebe preuzeti odgovornost za pristup osobnim podacima jer tvrde da su isti samo serviseri što je apsurd jer za ažuriranje i backupiranje trebaju dozvolu -akreditaciju za pristup istima. Kako bi se riješile nedoumice svaki odnos između voditelja i izvršitelja obrade osobnih podataka treba biti ugovorom definirano.

3.3 Ispitanik

Jednostavno rečeno ispitanik je svaka osoba, pojedinac, čiji se identitet utvrđuje, a osobni podaci obrađuju. Posebna kategorija su prava ispitanika koje poslovni subjekti trebaju štititi u skladu s navedenim načelima [17].

Prava ispitanika

Pravo na informaciju	Kategorije ispitanika koji imaju pravo na informiranje	Način objavljivanja informacije o pravu na zaštitu osobnih podatak
-**r**egulirana člankom 12. st. 1. Opće uredbe - obveza je voditelja obrade ispitanicima pružiti informacije iz članaka 13.-22. te 34	-radnici, kupci, dobavljači, partneri, korisnici usluga, učenici, studenti	-na web stranici, na oglasnoj ploči, uručivanjem ispitanicima ili na drugi način
-informacije treba pružiti u pisanom obliku, elektroničkim sredstvima ili u drugom prikladnom obliku		informacija mora biti lako pristupačna u svakom trenutku svakom ispitaniku
-način dokazivanja usklađenost svojeg sustava s Općom uredbom		

Opća uredba [1], u članku 12. st. 1. propisuje obvezu voditelja obrade da ispitanicima pruže informacije iz članaka 13.-22. te 34. Informacije se trebaju pružiti u pisanom obliku, elektroničkim sredstvima ili u drugom prikladnom obliku. Izvršenje ove obveze izuzetno je važno kako bi obveznik mogao dokazati usklađenost svojeg sustava s Općom uredbom.

Obveznici uvođenja Uredbe dužni su jednako informirati sve kategorije ispitanika (radnike, kupce, dobavljače, partnere, korisnike usluga, učenike, studente i dr.). Uredbom se zahtijeva da takvo informiranje bude u pisanom obliku, ali se ne određuje način objavljivanja takve informacije, pa se ona može objaviti na web stranici, na oglasnoj ploči, uručivanjem ispitanicima ili na drugi način. Bitno je da se nesumnjivo i na lako pristupačan način omogući svakom ispitaniku dostupnost takve informacije.

3.4 Privola ispitanika

O privoli je već dosta rečeno, a ovdje će se dati njezin sažetak [17].

Privola ispitanika

Definicija	**Upozorenje**	**Nedostatak**	**Primjeri u praksi kada privolu treba tražiti**
svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose	Ne smije biti uvjet za obavljanje ugovorenih aktivnosti	nerazumijevanje što je privola dovodi do prekomjernog prikupljanja podataka ili do izostanka privole tamo gdje je potrebna	snimanje, fotografiranje s točnom definiranom svrhom ovih radnji (npr. promidžba poslodavca objavom u sredstvima javnog informiranja itd.)

U praksi se često nailazi na jednu konfuziju po pitanju uporabe privola ispitanika za određene obrade, što dovodi do suvišnog administriranja i do nepotrebnog opterećivanja samih ispitanika. Razlog tome je nedovoljno poznavanje pravnog uređenja privole, kao pristanka na određenu radnju obrade osobnih podataka koju daje ispitanik.

Opća uredba određuje da je **obrada osobnih podataka zakonita** ako se **zasniva na najmanje jednoj od zakonitih osnova** navedenih u članku 6. st. 1., poglavlje 2.1.4.

Među definiranim osnovama privola je jedna od njih. Dakle, ako postoji neka druga od propisanih osnova, tada privola ispitanika nije nužna za zakonitost obrade. Primjerice, ako voditelj obrade mora određene osobne podatke prikupljati i obrađivati jer mu je takva obveza

propisana ili je nužna radi izvršenja nekog ugovora, tada mu za obradu osobnih podataka nije potreban pristanak ispitanika.

3.5 Obrada osobnih podataka

Obrada osobnih podataka znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje [1].

Obrada osobnih podataka u zdravstvene svrhe je neizbježna o čemu svjedoči bezbroj aktivnosti poput: pitanje javnog zdravlja, upravljanje uslugama zdravstvene skrbi, osiguranje kvalitete i isplativosti postupaka koji se upotrebljavaju za rješavanje potraživanja za naknadama i uslugama u sustavu zdravstvenog osiguranja ili u svrhe arhiviranja u javnom interesu, aktivnosti vezane za znanstvena ili povijesna istraživanja ili statističke svrhe.

Koliko je opsežna obrada osobnih podataka u zdravstvenoj djelatnosti može posvjedočiti tzv. evidencija aktivnosti obrade. Evidencija aktivnosti obrade višestruko je važan dokument. Ona je neizostavan dokaz usklađenosti sustava obrade osobnih podataka. Uz to, ona služi transparentnosti sustava obrade jer daje prikaz svih vrsta i načina obrade kod određenog obveznika.

Evidencija treba biti i sredstvo kojim će se obveznik služiti u rješavanju zahtjeva ispitanika, osobito zahtjeva za brisanje podataka. Također, u možebitnom nadzoru AZOP-a osobe ovlaštene za nadzor iz evidencije aktivnosti obrade steći će osnovna saznanja o postojanju i funkcioniranju sustava obrade osobnih podataka kod određenog obveznika.

Odredbom članka 30. st. 5. Opće uredbe određen je prag broja radnika (250 i više) prema kojem bi se određivala obveza vođenja evidencije aktivnosti obrade, iz čega obveznici s brojem radnika manjim od 250 zaključuju da nemaju obvezu vođenja te evidencije. Međutim, jedan od

izuzetaka koji se navodi u istoj odredbi (»ako obrada nije stalna«), upućuje na zaključak da ako obveznik provodi određenu stalnu obradu osobnih podataka, i ako su podaci koje obrađuju posebna kategorija osobnih podataka, dužan je voditi evidenciju aktivnosti obrade iako ima manje od 250 radnika. Jedan od takvih primjera su manji zdravstveni sustavi, primjerice privatne ordinacije i poliklinike s manje od 250 zaposlenika. [10] [17].

4. Pozitivni i negativni učinci Opće uredbe o zaštiti osobnih podataka na svakodnevni rad u zdravstvenom sustavu

U prethodnim poglavljima detaljno je objašnjena bit Uredbe o zaštiti osobnih podataka. Posebno su analizirana načela na kojima počiva Uredba jer su pomoću njih definirane uloge, odgovornosti i mehanizmi za primjenu zahtjeva Uredbe. Objašnjeni su organizacijski i tehnički zahtjevi koje Uredba postavlja ispred svakog zdravstvenog sustava bez obzira ne njegovu veličinu i složenost. Može se postaviti pitanje gdje je onda problem? Koliko god je prijašnji sustav ručnog unošenja i obrade osobnih podataka, njegovog arhiviranja i ponovnog pronalaženja bio problematičan zbog svoje sporosti i prekomjernog gomilanja papirnate dokumentacije za koju poslodavci više nisu raspolagali prostorom za njihovo fizičko odlaganje, danas se pojavio jedan novi problem, a to je „on line“ dostupan osobni podatak. Takav podatak u vrijeme brzog potraživanja i brze dostupnosti bitnih informacija za brzo donošenje odluka posebno u sferi liječenja zahtijeva od zdravstvenog sustava veće mjere informacijske sigurnosti nego što je to bilo unazad 20 godina. Upravo u ovom okruženju zdravstveni sustavi su se donekle snašli ili se uopće nisu snašli po pitanju zaštite osobnih podataka. O tome više u sljedećim poglavljima.

4.1 Zdravstveni informacijski sustav i Uredba

Stoljeće u kojem čovječanstvo djeluje obilježeno je četvrtom industrijskom revolucijom [18]. Ova značajka odnosi se na važnost informacije kao sredstvo i predmet rada. Neophodna sirovina za svakodnevnu obradu, planiranje poslovnih procesa, izvještavanje o rezultatima poslovnih procesa postaje upravo informacija - podatak. U mnoštvu podataka koji se svakodnevno obrađuju nalaze se i osobni podaci. Informatička tehnologija je velikim dijelom zaslužna za brzi prijenos, prihvat, obradu i pohranu neograničenog broja podataka pa tako i osobnih podataka pojedinca. Informatika je ostavila značajan trag u suvremenom životu i radu velikog broja ljudi. Pad cijene informatičke opreme i softvera omogućila je da računala postanu dostupna raznim poslovnim subjektima. Postoje mnogi zdravstveni sustavi, javni i privatni, koji desetljećima ulažu u informatičku tehnologiju bez koje je danas svakodnevni rad gotovo

nezamisliv. Nakon perioda otpora, prilagodbe i konačne primjene rad na računalima postaje normalna svakodnevica, radnici u svim sektorima ljudske djelatnosti postaju svjesni prednosti i olakšanja koja im stoje na raspolaganju.

U jednom zdravstvenom sustavu, primjerice sustav specijalističko konzilijarne zdravstvene zaštite, na dnevnoj osnovi obrađuju se stotine raznih podataka o osiguranicima, korisnicima zdravstvene usluge – pacijentima, dijagnostičko terapijskim postupcima i mnogi drugi koje je za neprekidan rad potrebno dnevno upisivati kako u ordinacijama tako i na svim ostalim radilištima koja su na izravan ili neizravan način uključeni u proces liječenja. Neke od njih treba dnevno, tjedno, mjesečno ili godišnje objedinjavati i ispisivati u obrasce koje redovito treba dostavljati u HZZO, HZJZ, Ministarstvo zdravstva, druge ustanove, osiguranicima ili drugim tražiteljima. Ono što je bitno u toj umreženoj izmjeni podataka je stvoriti standardizirane podatke, koje će biti lako upisivati, kontrolirati i obrađivati.

Na temelju dugogodišnjeg iskustva kolega iz stomatološke prakse, ali i iskustva samog autora ovog rada, način rada u specijalističko konzilijarnoj zdravstvenoj zaštiti dugo vremena je podrazumijevao veliku brigu o podacima, bez kojih ne može biti aktivnog pristupa osiguranicima. Ove aktivnosti provodila je isključivo medicinska sestra, u sklopu specijalističkog tima, svaka za svoj tim, pri čemu je ista brinula istovremeno i o «administraciji» i podacima i o bolesnicima. Uvođenjem informatizacije, stvari su se nešto bitnije promijenile u smislu automatske obrade i pohrane podataka o osiguranicima, međutim, medicinska sestra koja radi u timu s liječnikom specijalistom, i dalje je opterećena opsežnim administriranjem (bilježenje podataka o pacijentima i pruženim dijagnostičko terapijskim postupcima, brojne obveze u administriranju financijskih i knjigovodstvenih podataka, broj individualnih evidencija i obrazaca umnogostručio se). Na izgled idealna situacija u kojoj bi se više vremena posvećivalo samom osiguraniku, podrazumijevala bi provođenje takvih mjera i postupaka koji bi se oslanjali samo na upisu podataka u računalo, a koje bi prema pravilima i potrebama sami generirali podatke i izvještaje. Drugim riječima, ono što se očekuje od idealnog radnog okruženja, u eri digitalizacije svih podataka u zdravstvenom sustavu, je da računalo pomaže u bržoj transakciji svih postupaka i usluga, pri čemu bi izvješćivanje o istim podacima trebala biti posljedica rutinskoga rada, a ne poseban posao i aktivnost za timove.

U trenutku primjene informatičkih tehnologija naišlo se na veliki problem prilikom puštanja u rad određenih aplikacijskih rješenja s čijim su radom trebali nestati svi prethodni problemi.

Obrada podataka trebala je kontinuirano teći, tj. biti pravovremeno dostupna, potpuno automatizirana jednim klikom u bilo kojem trenutku, pronalaženje podataka o osiguranicima trebalo je biti brzo bez „pucanja“ veza s osiguravajućim kućama, mjesečna izvješća o ukupnosti rada tima trebali su biti dostupni bez dodatne evidencije, ručnog pronalaženja ili posebnih istraživanja.

Drugim riječima informacijski zdravstveni sustav predstavlja jedno složeno tijelo u kojem se digitalno obrađuju razno razni podaci, a između ostalih i osobni podaci. Složenost se posebno odnosi na razne uloge koje zainteresirane strane zauzimaju u takvom sustavu po pitanju autoriziranosti pristupa ovim osobnim podacima.

Sudionika koji na direktan i / ili indirektan način sudjeluju u pružanju zdravstvene usluge ima više. Ako se uzme da je Stomatološka poliklinika Zagreb u središtu takvog jednog zdravstvenog informacijskog sustava onda zainteresirane strane mogu biti [13]:

- specijalističko konzilijarni timovi,
- ordinacije primarne zdravstvene zaštite,
- zdravstveno osiguranje,
- javno zdravstvo,
- ministarstvo zdravstva,
- laboratoriji,
- bolnice,
- ostali zainteresirani subjekti itd.

U jednom ovakvom složenom sustavu potrebno je definirati sudionike u zdravstvenom informacijskom sustavu [13]:

- Medicinska sestra/administrator na prijemnom šalteru - autorizirani korisnik
  - unos podataka o bolesniku,
  - dodjeljivanje određenom specijalisti,
  - unos tražene pretrage,
  - unos u kompjuter - radnu stanicu, pohrana na serveru -poslužitelju,
- Liječnik specijalista- autorizirani korisnik
  - poslužitelj povratno isporučuju liječniku specijalisti podatke o bolesniku,

    - nakon obavljenog liječenja liječnik specijalist povratno upisuje i pohranjuje medicinsku dokumentaciju na poslužitelja ili ih printa putem pisača (povijest bolesti, nalazi, …),
- RTG dijagnostika, dentalni laboratorij, fakturisti, blagajna itd. – autorizirani korisnici,
- HZZO
    - sustav skladištenja podataka i izvještavanja – autorizirani korisnik,
- ostale zainteresirane ugovorene i autorizirane strane,
    - knjigovodstveno – računovodstveni servisi,
    - informatički servisi itd.

Kao što se može vidjeti iz prethodnog opisa za svaku pojedinu ulogu samo autorizirane osobe imaju pravo pristupa i pravo na obradu osobnih podataka. Na prvi pogled informacijski zdravstveni sustav djeluje puno jednostavnije, međutim, ciljevi koje isti postavlja pred sebe su puno složeniji posebno oni koji se odnose na svrhu digitalizacije podataka, pitanje sigurnosti tehničke, pravne i etičke prirode.

Kad je u pitanju digitalizacija podataka njezini ciljevi su višestruki [13]:

- tehnološka podrška (hardver i softver) i to svim postupcima pružanja svih usluga koje su na direktan i / ili indirektan način uključene u zdravstvene usluge,
- prenošenje informacija u zdravstvu,
- utvrđivanje potrebe za zdravstvenim i socijalnim uslugama,
- ispunjavanje visokih očekivanja građana u smislu dostupnosti zdravstvene usluge,
- organizacijske promjene i IT investicije,
- mobilnost pacijenta,
- kvaliteta zdravstvene usluge,
- unapređenje kvalitete sustava osiguranja,
- kontrola rada i praćenje kvalitete,
- mogućnost trenutnog saznanja o svim parametrima rada subjekata u zdravstvu,
- automatska obrada podataka,
- računalna obrada, pomoć pri odlučivanju,
- napredne usluge zdravstvenog osiguranja,
- uvođenje inteligentnih kartica pacijenata,

- interoperabilnost medicinskih podataka,
- ušteda resursa uvođenjem elektroničkih zdravstvenih kartona,
- svaka zdravstvena iskaznica ima jedinstveni broj pacijenta –smanjenje rizika od zamjene identiteta pacijenata,
- elektronički zahtjevi za naplatom troškova,
- automatizacija pri ažuriranju i dohvatu informacija o policama osiguranja,
- sigurnost na radu,
- upravljanje podacima,

Međutim, postavlja se pitanje sigurnosti i ovakve informacije [13].

Tehničko pitanje sigurnosti	**Pravno pitanje sigurnosti**	**Etičko pitanje sigurnosti**
• smanjenje broja pogrešaka • sigurna distribucija informacija i automatska obrada informacija • sprječavanje neovlaštenog pristupa ZIS-u • zaštita osobnih podatak • pravo na privatnost medicinskih podataka pacijenta/građana • vlasništvo zdravstvenog kartona – kontrola pristupa zdravstvenom kartonu (ovlaštenja)	• pravo na aktivno sudjelovanje u procesu liječenja i suodlučivanje na preporučeni dijagnostičko terapijski postupak u procesu –personaliziran pristup kartonu i javno zdravstvenim informacijama • povezanost – elektronička komunikacija sa svim entitetima sustava zdravstva	• poboljšanje kvalitete dijagnostike i procesa odlučivanja –korištenje zdravstvenih podataka središnjeg sustava • prava pacijenta na • informaciju • zaštitu privatnosti i dostojanstva • uvid u liječničku dokumentaciju

4.2 Osobni podaci u zdravstvenom sustavu

Uredba 2916/679, GDPR (engl. General Data Protection Regulation) [1], Zakon o provedbi opće uredbe o zaštiti osobnih podataka [2] – sinonimi su za zakonodavni okvir i smjernicu koja nedvosmisleno usmjeruje administrativne servise u svim poslovnim sustavima, pa tako i zdravstvenom prostoru, prvenstveno za informatičke i pravne aktivnosti, kako optimalno upravljati kategorijama osobnih podataka s aspekta vlasnika i izvršitelja obrade podataka.

Aktivacijom uredbe naglašava se važnost zaštite podataka u rastućem digitalnom svijetu što je stavilo iste u središte pozornosti tijela javnih zdravstvenih službi jer se radi o kategorijama posebno osjetljivih podataka te stoga ne čudi stalno naglašavanje aspekata zaštite, dostupnosti, potpunosti i odgovornosti.

Zdravstveno osoblje i pacijenti moraju imati potpuno jamstvo da se s njihovim osobnim i poslovnim podacima (koji tijekom obrade zdravstvenog slučaja postaju povjerljive poslovne informacije) postupa kroz kontroliranu poslovnu politiku, u skladu sa zakonom, etičkim kodeksom i poslovnim moralom. Ovakav savjestan pristup bio bi nemoguć bez adekvatne IT (engl. information technology) i operativne platforme i stručnjaka iz područja unutar sustava zdravstva.

Stručnjaci iz područja IT-a u sustavu zdravstva stavili su pred sebe poseban izazov u pogledu standardizacije osobnih podataka ili općenito podataka koji se svakodnevno obrađuju u zdravstvenom sustavu. Podaci koje jedna npr. specijalističko konzilijarna ordinacija dentalne medicine treba prikupljati obuhvaća bilježenje uobičajenih događaja/transakcija po svakom posjetu/pregledu/liječenju koje bi u budućim događajima u kratkom vremenu dobila mnogo kvalitativnih informacija za nastavak liječenja. Iste transakcije informacija ne služe samo navedenoj ordinaciji, tj. poslodavcu u sklopu kojeg ordinacija djeluje, nego bi trebale biti usklađene sa standardiziranim podacima koje na isti način obrađuje i HZZO, HZJZ, ostali korisnici na način da mnogi podaci o raznim aktivnostima budu adekvatno bilježeni i fakturirani. Očekuje se da obrada podataka od strane svih korisnika bude na kopijama istih podataka (istim bazama), obrasci i izvješća trebala bi se automatski generirati kako se specijalistički timovi ne bi trebali brinuti o istima već se isključivo baviti svojim poslom.

Ovakav pristup digitalizacije podataka i standardizacije podataka trebao bi dovesti do, možda ne nestanka, ali barem smanjenja grešaka/razlika koje nastaju kod ručnog unošenja podataka [15].

Kad se već spominje standardizacija podataka koji se obrađuju u zdravstvenom sustavu treba posebno definirati koji su to osobni podaci, tj. posebne kategorije osobnih podataka. Pa tako Uredba posebno navodi proširenje pojma osobnog podatka u području zdravstva [14] podatak koji se odnosi na zdravlje fizičke osobe: osobni podatak koji se odnosi na tjelesno ili mentalno zdravlje fizičke osobe, uključujući pružanje zdravstvenih usluga koje otkrivaju informacije o zdravstvenom statusu fizičke osobe

- genetički podatak: osobni podaci koji se odnose na naslijeđena ili stečena genska obilježja fizičke osobe, koja daju jedinstvenu informaciju o fiziologiji ili zdravlju te fizičke osobe i koja proizlaze iz analize biološkog uzorka fizičke osobe o kojoj je riječ,
- biometrijski podatak: osobni podatak koji proizlazi iz specifične tehničke obradbe koja se odnosi na fizičke, fiziološke ili bihevioralne karakteristike fizičke osobe, a koje dopuštaju ili potvrđuju jedinstvenu identifikaciju te fizičke osobe (npr. slika lica, otisak prsta...

Upravo zato Uredba u području zdravstva pooštrava definiciju osobnoga podatka i zahtijeva zaštitu integriteta, povjerljivost i zaštitu neovlaštene dostupnosti osobnih podataka, osim u izvanrednim situacijama i to [1]:

- onaj koji obrađuje osobne podatke mora imati „eksplicitni pristanak“ osobe da se koristi njegovim podatcima,
- ukoliko je obrada osobnih podataka nužna u svrhu preventivne ili profesionalne medicine, za procjenu radne sposobnosti zaposlenika, medicinsku dijagnozu, pružanje zdravstvene ili socijalne skrbi ili liječenje ili upravljanje sustavima i uslugama zdravstvene zaštite ili socijalne skrbi,
- obrada je potrebna iz razloga javnog interesa u području javnoga zdravstva, kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju ili osiguranje visokih standarda kvalitete i sigurnosti zdravstvene zaštite te lijekova ili medicinskih proizvoda.

U svim ostalim slučajevima, osobni podatak koji zdravstvena ustanova posjeduje, ne smije se obrađivati. Uredba govori o „pristanku“ na obradu osobnih podataka, a u području zdravstva govori se o „eksplicitnom pristanku“ što je pooštrenje zahtjeva.

Osobni podaci koji se obrađuju u zdravstvenom sustavu mogu se podijeliti u dvije skupine [13]:

Osobni podaci korisnika zdravstvenih usluga -pacijenata	**Osobni podaci tzv. zdravstvenih resursa - radnika**
•ime i prezime, •OIB, •datim rođenje, •adresa stanovanja, •zdravstveno osiguranje: ime i prezime pacijenta, broj police osiguranja, OIB pacijenta, •osnovno i dopunsko, •osiguravajuće društvo , •podaci o zdravstvenom stanju pacijenta: dohvat/unos medicinskih podataka iz/u središnju arhivu zdravstvenih kartona pacijenata: HZZO – CEZIH, HZJZ- NAJS, e-građanin, •tegobe, simptomi,... •rezultati pregleda, dijagnostičkih i lab. pretraga, ... •dijagnoza ili opis problema/stanja •terapija, upućivanje, naručivanje na kontrolni pregled, •popis lijekova koje pacijent koristi •alergije na lijek •bolesnici s kroničnim bolestima •zarazne bolesti, itd.	•ime i prezime liječnika specijalista koji je pružio uslugu i koji ima šifru za pristup u CEZIH (centralni zdravstveni informacijski sustav), •šifra dijagnostičko terapijskog postupka, •šifra utrošenog stomatološkog materijala, •normativ DTP-ova (dijagnostičko terapijskih postupaka) itd., •broj uputnica za PHD (patohistološku dijagnozu) nalaz, •materijali trošak, •itd.

U poglavlju 2. često se navodio pravni temelj za prikupljanje i daljnju obradu osobnih podataka, Na primjeru dentalne medicine ove aktivnosti se provode kao zakonska obaveza voditelja zbirke osobnih podataka, voditelj je poslodavac zdravstvenog sustava, i to putem:

- ako je obrada propisana zakonom [20]:
  - Zakon o dentalnoj medicini (NN 121/03, 117/08, 120/09)
  - Zakon o pravu na pristup informacijama (NN 25/13, 85/15)
  - Zakon o zaštiti osobnih podataka(NN 106/12)
  - Zakon o zaštiti prava pacijenata(NN 169/04, 37/08)
  - Zakon o zdravstvenoj zaštiti(NN 100/18)
  - Zakon o obveznom zdravstvenom osiguranju(NN 150/08,,139/10)
  - Zakon o kvaliteti zdravstvene zaštite i socijalne skrbi(NN124/11)
  - Zakon o evidencijama u oblasti zdravstva (SL SFRJ 22/78, 18/88, NN 53/91, 26/93, 29/94)
  - Zakon o radu (NN 93/14), itd.
  - Pravilnik o načinu vođenja, čuvanja, prikupljanja i raspolaganja medicinskom dokumentacijom pacijenata u Centralnom informacijskom sustavu zdravstva Republike Hrvatske(NN 82/10)
  - Pravilnik o načinu vođenja osobnog zdravstvenog kartona u elektroničkom obliku(NN 82/10itd.
- sklapanjem i izvršenje ugovora u kojem je osoba čiji se podaci obrađuju jedna od ugovornih strana,
  - ugovori o radu s radnicima, pripravnicima, učenicima na praksi i ostalim osobama koji su na bilo koji način u radnom odnosu u Poliklinici,
- ispunjenjem zadataka koji se izvršavaju u javnom interesu ili u izvršavanju javnih ovlasti koje ima voditelj zbirke osobnih podataka,
- zakonitim interesom voditelja zbirke ili treće strane kojoj se podaci daju na korištenje [13],
  - Poslodavac i HZZO
  - Poslodavac i FINA
  - Poslodavac i Ministarstvo Zdravstva,
  - Poslodavaca i njezin osnivač,

- ako je obrada nužna radi zaštite života ili tjelesnog integriteta osobe čiji se podaci obrađuju ili druge osobe kada ona fizički ili pravno nije mogućnosti dati svoj pristanak na takvu obradu
- privola osobe čiji se podaci obrađuju,
    - pisani pristanak pacijenta na obradu njegovih podataka u točno određene svrhe
    - pacijentov sporazum mora se temeljiti na točnom razumijevanju razloga obrade
    - pacijent ima slobodu izbora i povlačenja pristanka, a informacije se koriste samo u svrhe u koje je dano
        - primjer: objava osobnih fotografija u dentalnom vjesniku, web stranicama, sudjelovanje u znanstvenim istraživanjima
    - privola potpisana od radnika u svrhe marketinga poslodavca,
    - privola potpisana od radnika u svrhu praćenja kretanja službenog auta putem GPS-a, itd.
- ako je osoba sama objavila svoje podatke.

Zaključno, u dentalnoj medicini, jasno je da je relevantan „pravni temelj“ obrade podataka nužan preduvjet za pružanje specijalističke usluge od strane registriranog stomatološkog stručnjaka.

4.3 Organizacijske i tehničke mjere zaštite osobnih podataka

Kao što je u poglavlju 3. navedeno digitalizacija podataka u zdravstvenom informacijskom sustavu ima za cilj osigurati nesmetan i kontinuiran rad poslovnog sustava kako bi se izbjegao zastoj sustava ili u najgorem slučaju gubitak informacija, a što predstavlja sigurnosni incident u području zaštite osobnih podataka. Primjera radi, hakiranje podataka u kadrovskoj službi, podataka na blagajni, podataka u računovodstveno-knjigovodstvenoj službi itd. predstavlja sigurnosni incident o kojima AZOP mora biti obaviješten u pisanom obliku u roku 72 sata od trenutka saznanja o incidentu [1] [2].

Upravo je analiza rizika, kako je navedeno u poglavlju 2.1.1, važna kako bi se predvidjeli mogući incidenti u procesima prikupljanja, održavanja, pohranjivanja, čuvanja i obrade podataka jer je obveznik Uredbe odgovoran za iste pred zakonom.

Dakle, u svim zdravstvenim sustavima svakodnevno se provodi više vrsta obrada osobnih podatak poput [13]:

- skupljanje podataka,
- obrada podataka,
- pohrana podataka,
- osiguranje zaštite podataka i informacije u zdravstvu od neovlaštenog pristupa,
- osiguranje uvida u podatke i informacije u zdravstvu samo ovlaštenim djelatnicima i korisnicima zdravstvenog informacijskog sustava.

Nastavno za zadnje, preduvjet pristupa osobnim podacima podrazumijeva definiranje procesa autorizacije i autentifikacije, tj. procesa prepoznavanja korisničkog identiteta kojim se pristupa podacima. Svrha definiranja ovih procesa je kontrola na kojim pravnim i poslovnim osnovama vlasnik obrade podataka prikuplja, obrađuje i čuva osobne podatke korisnika, da bi u konačnosti kao informacija mogli biti uvijek dostupni u poslovnim procesima. Tako se zakonski uvjetuje transparentan proces obrade podataka u kojem su privola osobe, poslovni ugovor ili javni interes temeljeni na zakonu jedini dopušteni okviri za buduće obrade osobnih podataka.

4.3.1 Organizacijske mjere zaštite osobnih podataka

Pacijent kao vlasnik svojih osobnih podataka, jednom kada uđe u zdravstveni sustav mora znati da u zdravstvenim ustanovama postoje kvalitetne strukture (oprema i ljudi) koji znanjem i kompetencijama upravljaju složenim poslovnim procesima u zdravstvenom prostoru. Iako je Uredba prvenstveno pravno pitanje istu je nemoguće provesti bez integracije s IT rješenjem. Uredba stoga zahtjeva definiranje organizacijskih i tehničkih mjera zaštite osobnih podataka koje moraju krajnjem korisniku na transparentan način dati do znanja da je zdravstvena ustanova u kojoj dolazi po određenu uslugu sukladna s Uredbom [1] [2] [15].

Odgovornost voditelja obrade vidi se u preuzimanju odgovornosti za poduzete radnje po pitanju zaštite osobnih podataka. Odgovornost voditelja obrade može se promatrati kroz [13]:

- organizacijske mjere koje podrazumijevaju:
  - dostupnost podataka,
  - jasnu svrhu prikupljanja osobnih podataka,
  - obradu podataka samo unutar unaprijed dogovorenog konteksta,
  - definiranje kompetentnih radnika koji se brinu o podacima,
  - sustav za upravljanje dokumentacijom o privolama,
  - nadzor nad sustavom obrade podataka,
  - pravilnici, smjernice, zapisnici,
  - postojanje dokumentacije o obradama podataka - protokoli te konačno
- tehničke mjere poput:
  - autorizacija i autentifikacija tj. što tko može i smije raditi,.

Opravdanje za uspostavu ovih mjera leži u potencijalnom riziku od malicioznih pojava zbog čega voditelj obrade mora provesti dobro osmišljen i koncipiran sustav upravljanja. Počevši od ljudskog potencijala za optimalno nadziranje rada sustava uz pomoć dostupne tehnologije do dokumentiranja poslova izvršenja poslovnih procesa pomoću IT sustava u skladu sa zahtjevima EU uredbe [1] [6] [8]. Potencijalni rizik poslovanja zdravstvenog sustava, rizik od gubitka podataka, zahtjeva veću odgovornost i sankcioniranje voditelja obrade za loše odrađeni posao u bilo kojoj profesionalnoj domeni, što vrijedi za sve struke koordinirane u procesu obrade podataka, bilo da su zadužene za pravnu dokumentaciju u procesu ili nadzor kvalitete provedbe u poslovnim procesima.

4.3.2 Tehničke mjere zaštite osobnih podataka

Tehničke mjere zaštite odnose se prvenstveno na mjere sigurnosti u informatički sustav. One se kreću od fizičko-tehničke zaštite prostora s poslužiteljskom informatičkom opremom do sustava autoriziranog i kontroliranog osiguranja stalnog pristupa bazama osobnih podataka. Međutim, tehničke mjere zaštite nemoguće je promatrati bez organizacijskih i operativnih mjera zaštite u informatičko-telekomunikacijskom sustavu. Svaka od ovih aktivnosti zahtijeva stalno

održavanje, nadogradnju, testiranje i nadzor svih aktivnosti u poslovnom informatičkom procesu pri čemu glavnu ulogu nosi čovjek ili kao administrator ili kao onaj kojemu su dodijeljene akreditacije.

Praksa je pokazala da ne postoje apsolutno pouzdana informatička rješenja. Počevši od same opreme koju treba obnavljati u nekom razumnom periodu. Zatim, zastoj u prijenosu podataka može biti potencijalni incidentni događaj jer u zdravstvenom sustavu zastoj u prijenosu osobnih podatak je neželjeni događaj. Osim zastoja može biti u pitanju i gubitak osobnih podataka pri čemu uzroci problema tehnološke prirode mogu biti razni te stoga tehnička mjera zahtjeva postojanje kvalitetne kopije podataka, jamstva da je ona ispravna, a ako se to radi na posebno osjetljivim radilištima, tada valja imati i pričuvni položaj za nastavak rada u slučaju ispada primarne lokacije. Zbog toga se radi i procjena rizika s obzirom na sve elementarne nepogode koje se mogu pojaviti u informatičkom prostoru.

Uređaj za neprekidno napajanje, ili prijenosnik s ispravnom baterijom, mora osigurati da podaci unutar transakcijskog procesa budu uvijek zapisani na medij za pohranu podataka, čak i u slučaju nestanka struje. Najčešće rješenje za takve situacije je odabir novog mjesta baze podataka u tzv. „Podatkovnom centru“ ili „Oblaku“. Međutim, i u slučaju takvih rješenja administrator informatičkog sustava treba točno navesti gdje se tzv. „Oblak“ nalazi. Nebriga i nemar u informatici od strane administratora, ali i voditelja obrade jer ih je na osnovi ugovora ovlastio kao izvršitelje obrade, također podliježu sankcioniranju.

U nastavku teksta manje će se pisati o tehničkoj prirodi samog informatičkog mehanizma i strategiji paralelnog zapisa na dvije lokacije kao i o periodičnom mijenjanju diskova prije njihovog optimalnog roka trajanja jer je to zdravstvenim praktičarima manje blisko područje.

Zdravstvenim praktičarima mora biti jasno da Uredba donosi jasnu spoznaju da su zdravstveni podaci u malim i velikim sustavima iznimno važna „roba“ i da se prema njima treba ponašati s dužnim poštovanjem jer su postali predmet zaštite uređene zakonom.

Svaki zdravstveni praktičar, pa i svi oni koji na indirektan način obrađuju osobne podatke bilo pacijenata ili radnika moraju znati da se svaka transakcija osobnih podataka nastala u zdravstvenom prostoru Hrvatske pohranjuje u CEZIH-u (Centralni zdravstveni informacijski

sustav Republike Hrvatske), centralni repozitorij svih medicinskih podataka, nastalih na svim razinama zdravstvene zaštite. Osim što je to središnje mjesto gdje se slijevaju podaci sa svih razina, CEZIH je i on-line zaštita podataka u realnom vremenu, na još jednoj lokaciji, koja je apsolutno tehnološki sigurna od kvara i zastoja. Isto vrijedi i za NAJS (Nacionalni javnozdravstveni informacijski sustav) i za sustav e-građanin. Koncepcija izrade elektroničkog zdravstvenog zapisa je rješenje koje donosi sve komparativne prednosti digitalne ekonomije, pa tako i u zdravstvenom prostoru [15].

Zakonom o podacima i informacijama u zdravstvu [15] predviđen je rok od 5 godina potpune digitalizacije svih podataka iz zdravstvene djelatnosti koji će se prikupljati u jedinstvenu bazu podataka za sve osiguranike u Hrvatskoj i obrađivati elektronski. Može se postaviti pitanje osiguranja potrebnih sredstava kako bi se zahtjevi raznih zakona i pratećih propisa zadovoljili i zaštitilo poslodavca od eventualnog kaznenog progona.

Informatizacija zdravstvenog sustav podrazumijeva nabavu informatičke opreme za sve timove, i prateće djelatnosti koje na direktna ili indirektan način sudjeluju u dijagnostičko terapijskim postupcima. Korist od uvođenja informatizacije zdravstvenog sustava bila bi poboljšanje ukupne skrbi za bolesnike i osiguranike, povećanje brzine u dijagnosticiranju i određivanju terapije, bolje iskorištavanje kapaciteta, smanjivanje vremena čekanja, skraćivanje vremena provedenog u zdravstvenim ustanovama, osiguranje jednakosti u dobivanju brze i kvalitetne skrbi za sve osiguranike [15].

Pitanje tehničkih mjera zaštite osobnih podataka podrazumijeva:

- uvođenje magnetskih iskaznica osiguranika,
- uvođenje elektronskih smart kartica za sve doktore u sustavu zdravstva,
- kod svakog pregleda ili prijama u bolnicu istodobno se provjerava i status i prava kako osiguranika tako i doktora
- «spajanjem» magnetske kartice osiguranika i smart kartice doktora omogućava se trenutna transakcija podataka,
- dostavu laboratorijskih i drugih nalaza (RTG snimke itd.) u elektronskom obliku, u realnom vremenu specijalisti

- automatsko spremanje svih nalaza u elektronsku «košuljicu/karton» osiguranika i da ovlaštenim doktorima i pacijentu budu uvijek dostupni kao osnova za evaluaciju rezultata u zdravstvenoj zaštiti.

Tehnička mjera zaštite osobnih podataka obuhvaća autorizaciju pristupa osobnim podacima, tj. davanje autorizacije za kontrolirani pristup podacima mora biti u skladu s opisom poslova u sistematizaciji radnih mjesta. Dodjelu autorizacije provodi administrator aplikacije. Njegova glavna zadaća je upravljanje akreditacijama i vjerodajnicama za pristup podacima djelatnika u poslovnom sustavu. Zašto? Zato što podaci u zdravstvenom prostoru uz informatički podržane procesne obrade, u pravom trenutku, na pravome mjestu, u rukama zdravstvenog osoblja postaju optimalno korisne informacije.

Zdravstveno osoblje izvodi operativne radnje na temelju raspoloživosti podataka kroz informatičku tehnologiju.

Na primjer, pojedinac na određenom radnom mjestu – primjerice radnik na prijemnom šalteru, osoba koja provodi evidenciju prijema pacijenta na temelju uputnice i dodjelu određenom specijalističko konzilijarnom timu, samo u pojedinom slučaju mora biti upoznata s osobnim podacima osobe koja je zatražila određenu specijalističku uslugu. Zato dobiva akreditaciju za taj dio posla. Ukoliko to opisom poslova u sistematizaciji radnih mjesta nije predviđeno ovaj radnik na prijemnom šalteru nikada ne smije imati generički uvid u medicinsku dokumentaciju svih pacijenata koji su pristupili tom specijalističkom odjelu ili svim odjelima zdravstvene ustanove. Međutim, još uvijek se u praksi susreću želje voditelja specijalističkih odjela za povećanja opsega obrade osobnih podataka radnika na šalteru samo da bi se specijalistički timovi rasteretili i one preostale administracije koja je u opisu njihovog radnog mjesta. Ovdje je velika odgovornost na administratoru informatičkog sustava koji dodjelu ovlaštenje i odobrenje daje isključivo u pisanom obliku po nalogu voditelja odjela. Bitno je naglasiti da jednom dodijeljena autorizacija radniku prati svaku njegovu aktivnost popit pisanja, čitanja, ažuriranja, brisanja podataka uz točno navođenje razloga za takvim aktivnostima.
Na točno određenom specijalističkom odjelu podaci o trenutačnom broju pacijenata koji čekaju na uslugu dostupni su liječnicima akreditiranima na toj fizičkoj lokaciji. Ako postoji potreba za konzilijarnim pregledom, liječnika s druge fizičke lokacije mora se ovlastiti za pristup podacima pacijenta koji je predmet medicinske obrade. Otvaranjem elektroničkog radnog naloga taj se protokol ponašanja otvara automatizmom.

Znaju li pacijenti ili ne da se pristup njihovim podacima mora akreditirati, nije poznati, ali zato je ovaj zahtjev utkan u EU uredbi upravo kako bi se zaštitili medicinski podaci od neovlaštenog pristupa.

Uredba bi kod pacijenta trebala podignuti svijest o pravu na privatnost osobnih podataka. Ne samo kod njega nego i na svim razinama obrade osobnih podataka u zdravstvenoj ustanovi. Od djelatnika na prijemnom šalteru, na pultu za informacije, zdravstvenog osoblja, ljudi u obračunu, fakturama, računovodstvu, uredu za podnošenje žalbi do same informatičke službe koja ne može automatizmom raspolagati informacijama o pacijentima i zaposlenicima unutar zdravstvene ustanove.

Zato je za obradu i pristup osobnim podacima na svim razinama potrebna je akreditacija. To je bit zakona o zaštiti osobnih podataka. Onaj koji daje akreditaciju je sam korisnik zdravstvene zaštite koji svojim traženjem usluge u datom trenutku, na određenom odjelu od određenog specijalističkog tima akreditira upravo tog specijalistu kako bi ovaj pristupio njegovim podacima s jasnom svrhom i ciljem, i to na temelju digitalne isprave i s digitalnim certifikatom.

Dakle, s jedne strane je pacijent koji akreditira specijalistu za pristup njegovim osobnim podacima, a s druge strane je administrator zdravstvenog informacijskog sustava koji na temelju vjerodajnica, digitalnog certifikata, daje specijalisti dozvolu za pristup osobnim podacima pacijenta. Nažalost, na pojedinim radilištima još uvijek je prisutan sustav identifikacije kroz korisničko ime i zaporku koji se pokazao kao jako rizično rješenje. Ako se tome dodaju vjerodajnice ispisane na papiru i zalijepljene na okvir ekrana računala onda ni najsuvremenija tehnička mjera zaštite osobnih podataka ne drži vodu. Trebalo bi biti svima jasno da takav pristup zaštiti osobnih podataka ukazuje na neozbiljnost, nepouzdanost i neodgovornost voditelja obrade. Jedino sigurnim sustavom zaštite osobnih podataka smatra se identifikacijom pomoću digitalnih certifikata. Pomoću digitalnih certifikata ne samo da se određuje na kojim lokacijama osoba može raditi, koje joj je osnovno radilište, koje uloge i role su pridodane poput prava nad aktivnostima u radu s podacima, već se i prate sve aktivnosti u informatičkom sustavu jer su svi korisnici akreditirani. To znači da se korisničko ime i zaporka za pristup sustavu ne smiju ustupiti nikome. Vjerodajnice su korisnikovo osobno vlasništvo, parametri koji ga identificiraju u digitalnom svijetu, i on je odgovoran na svim razinama gdje se pojave ti identifikatori. Tko pristupa u sustav, tko ima prava na kojem radilištu, kojim dokumentima se

može pristupiti, tko je autor podataka, tko ih ažurira, tko je odgovoran za opravdano i neopravdano brisanje podataka, tko čita podatke, sve se to bilježi u posebnom paralelnom dnevniku radu. I identifikacija zapisa se provodi na temelju vjerodajnica. Stoga je vjerodajnice potrebno iznimno dobro čuvati, one su u digitalnom svijetu osobno vlasništvo i odgovornost te je briga o njima neprocjenjiva!

Jedno od mogućih tehničkih mjera zaštite osobnih podataka predstavlja pseudonimizaciju, anonimizaciju i / ili kriptiranje osobnih podataka s ciljem smanjivanja štetnih posljedica neovlaštenih ili neautoriziranih ulazaka u zonu osobnih i poslovnih podataka. Jasno je da bankarski sustavi imaju ovakve tehničke mjere zaštite osobnih podataka i zbog posjedovanja značajnih financijskih sredstava za provedbu ovakvih mjera. Međutim, imaju li zdravstvene ustanove dovoljno sredstava za primjenu istih zaštitnih mjera???

4.4 Učinci Opće uredbe o zaštiti osobnih podataka na svakodnevnu praksu u zdravstvenom sustavu

Opća uredba o zaštiti podataka (GDPR) dočekana je kao veliki poremećaj u poslovanju mnogih tvrtki jer su njezini zahtjevi od 25. svibnja 2018. godine imali za cilj drastično povećati transparentnost u načinima obrade podataka bilo koje tvrtke koja obrađuje podatke građana EU-a. Kao 'predmetu obrade', građanima EU-a je omogućena veća kontrola nad vlastitim podacima, donošenje odluka o tome tko će ih koristiti i kako ih te tvrtke mogu koristiti. Kad je zdravstveni sustav u pitanju, zbog svega prethodnog navedenog, ovdje se može govoriti o prednostima i nedostacima primjene uredbe u svakodnevnoj praksi zdravstvenog sustava pa tako i o njezinim različitim učincima.

4.4.1. Prednosti primjene Uredbe i njezini pozitivni učinci

- Pravna usklađenost

Pridržavanjem i implementacijom načela Uredbe postižu se zaštitni mehanizmi od mogućih novčanih kazni.

- Poboljšano povjerenje ispitanika - korisnika zdravstvene zaštite

Pridržavanjem zahtjeva Uredbe ispitanicima se dokazuje da je zdravstvena organizacija dobar čuvar podataka. Imenovanjem službenika za zaštitu podataka (DPO – eng. Data Protection officer) provode se redoviti auditi i revizija aktivnosti obrade podataka.

- Bolje upravljanje poslovanjem

Poštivanjem zahtjeva Uredbe dovodi se boljih poslovnih praksi i očuvanja ugleda zdravstvene ustanove.

- Bolja sigurnost podataka

Kršenje cyber sigurnosti predstavlja veliku prijetnju za zdravstvene sustave. S obzirom na razmjer i sofisticiranost ovih napada zahtjevi u skladu s Uredbom nameću višu razinu informacijske sigurnosti. Uredba zahtjeva definiranje procedura dodjele akreditacija za pristup osobnim podacima samo onim profesionalcima koji imaju pravo na njihovu obradu.

- Bolje usklađivanje s novom tehnologijom

Poboljšanjem sigurnosti mreže, krajnjih točaka i aplikacija, prelaskom na najnovije tehnologije - virtualizaciju, računalstvo u oblaku itd. zdravstvena organizacija može stalno pratiti svoje novo okruženje za bilo kakvo kršenje podataka. I to pomoću dnevnika podataka, provjerom integriteta datoteka i mapa u zdravstvenoj ustanovi, na krajnjim uređajima i aplikacijama, kao i u oblaku.

- Promjena kulture zaposlenika – podizanja svijesti o odgovornosti

Podizanje svijesti o zaštiti i sigurnosti osobnih podataka koje svakodnevno obrađuju i to edukacijom o obradi podataka kao zakonitoj obradi, za posebne i jasne svrhe, točnoj obradi, dostupnoj i dovoljnoj za dovršavanje zadataka, sigurno rukovanje i ne pretjerano za postizanje svrhe. Promjena kulture zaposlenika podrazumijeva i podizanje svijesti o transparentnosti i odgovornosti, o zaštiti osobnih podataka u svojim procjenama rizika i potencijalnom riziku od novčanih kazni i gubitku ugleda poslodavca.

4.4.2 Nedostaci primjene Uredbe i njezini negativni učinci

- Strogo čuvanje podataka

Od svake tvrtke pa tako i od zdravstvene organizacije očekuje se strogo pridržavanje načela po pitanju čuvanja i održavanja osobnih podataka tj. strogo pridržavanje slova zakona a da se pri tome ne gleda financijska sposobnost i kadrovska raspoloživost zdravstvene organizacije da provede sve te mjere. Rezultat toga je prepisivanje politika o zaštiti osobnih podataka s interneta što često nema veze sa stvarnom praksom.

- Trošak

Sve aktivnosti uz organizaciju, provedbu, edukaciju, primjenu organizacijskih i tehničkih zaštitnih mjera imaju svoju cijenu te svi zdravstveni sustavi, i veliki i mali, trpe zbog ovih izvanrednih i neplaniranih troškova. Troškovi postizanja usklađenosti mogu varirati od stotina eura do desetak tisuća eura. Nejasnoća propisa zahtijevala je da zdravstvene organizacije angažiraju skupe odvjetnike koji opet ne poznaju sustav.

- Edukacija

U velikim zdravstvenim sustavima traje dugo, zahtijeva prethodno osposobljavanje stručnog kadra za edukaciju o Uredbi.

- Postupci zaštite podataka

Podrazumijeva sve raspoložive organizacijske i tehničke zaštitne mjere koje imaju svoju cijenu. Iako sustav raspolaže najnovijim čudima moderne tehnologije po pitanju informacijske sigurnosti još uvijek se neozbiljno pristupa zaštiti osobnih podataka po pitanju zaštite dodijeljenih akreditacija.

- Ljudski faktor

Uvijek je čovjek najslabija karika. Potpisivanjem izjave o povjerljivosti osobnih podataka ne garantira se 100 % informacijska sigurnost.

5. Zaključak

Vlasnik obrade podataka je glavna i odgovorna osoba za procese obrade podataka i kao takva u slučaju bilo kakvog incidenta jedini krivac. Pojam odgovornosti sada je dobio na težini. EU Uredba poručuje da se valja profesionalno odnositi sa svim elementima informatičkog kruga, posebno podacima. Mehanizmi za zaštitu pristupa podacima, dokumentima, bazama podataka, kriptiranje sadržaja i dizajn baze podataka – u središtu su pozornosti EU uredbe.

Praksa uči kako je uvijek čovjek ta najslabija karika. Stoga stalnom edukacijom o važnosti zaštite, preuzimanjem odgovornosti u slučaju nastanka incidentnih događaja te procjenom rizika trebalo bi pronaći slabe točke u aktualnoj strukturi kada su u pitanju sigurnosni i operativni problemi u procesima obrade medicinskih podataka.

Literatura

[1] Uredba (EU) broj 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

[2] Zakon o provedbi Opće uredbe („Narodne novine“, broj 42, 2018)

[3] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL L 281, 23.11.1995., str. 31.)

[4] Special Eurobarometer 487a – March 2019, “The General Data Protection Regulation”, Report, DS-04-19-461-EN-N, ISBN 978-92-76-08384-9, Dostupno: http://ec.europa.eu/commfrontoffice/publicopinion

[5] Direktiva 2011/24/EU Europskog parlamenta i Vijeća od 9. ožujka 2011. o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi (SL L 88, 4.4.2011., str. 45.)

[6] Uredba (EZ) br. 1338/2008 Europskog parlamenta i Vijeća od 16. prosinca 2008. o statističkim podacima Zajednice o javnom zdravlju i zdravlju i sigurnosti na radnom mjestu (SL L 354, 31.12.2008., str. 70.)

[7] Direktiva 2003/98/EZ Europskog parlamenta i Vijeća od 17. studenoga 2003. o ponovnoj uporabi informacija javnog sektora (SL L 345, 31.12.2003., str. 90.)

[8] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.)

[9] https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

[10] Šimunec, N. Neka pitanja o implementaciji Opće uredbe o zaštiti podataka, Informator, broj 6551, 2018

[11] Hrvatska komora dentalne medicine, Dostupno na: https;//www.hkdm.hr: Kodeks dentalne etike i deontologije

[12] Stomatološka poliklinika Zagreb, Dostupno na: https://www.spz.hr.dokumenti

[13] Krstić Vukelja, E: Opća uredba o zaštiti osobnih podataka u svakodnevnoj praksi, Program edukacije zaposlenika Stomatološke poliklinike Zagreb, 2019.

[14] Armstrong, J.P; Bywater, A: What healthcare organizations should know about GDPR, Absolute Software Corporation, 2017.

[15] Krstić Vukelja, E.; M., Vukelja: Neka objašnjenja pojmova iz uredbe o zaštiti osobnih podataka,Vijesnik dentalne medicine, br. 1, pp. 13-18, ožujak 2019.

[16] Zakon o zaštiti prava pacijenata, („Narodne novine“, broj 37, 2008)

[17] Zakon o podacima i informacijama u zdravstvu („Narodne novine“, broj. 14, 2019)

[18] Krstić Vukeja, E: Osobna menadžerska filozofija promjena u zdravstvu s osvrtom na pametna poduzeća, Seminarski rad, Libertas, 20217.

[19] Markovinović N. GDPR-izazovi za menadžere i poslovne analitičare. Kontroling, financije, menadžment. 2017;4.

[20] Hrvatska komora dentalne medicine, Dostupno: https://hkdm.hr.dokumenti

Sažetak

Uredba (EU) 2016/679 Europskog parlamenta i vijeća predstavlja velik iskorak u području zaštite osobnih podatka i informacijske sigurnosti jer je nastala kao rezultat nedovoljno učinkovitog prethodnog nacionalnog zakonodavstva u području uređenja virtualnog okruženja i zaštite prava građana EU u pogledu obrade njihovih osobnih podataka. Razvoj ljudskih djelatnosti u digitalnom svijetu povlači za sobom ubrzani razvoj informacijskih i komunikacijskih tehnologija, a istodobno stvara nove izazove i ugroze privatnosti i zaštite osobnih podataka. Obrada podataka, osobito obrada posebnih kategorija osobnih podataka poput zdravstvenih podataka, novi IT alati i digitalno tržište, razvilo je potrebu za povećanjem zaštite privatnosti novih digitalnih proizvoda i usluga pomoću kojih se ove kategorije osobnih podataka obrađuju te se uvođenje Uredbe u obaveznu praksu smatra opravdanim.

Uredba bi trebala osigurati ujednačeno postupanje u procesu obrade osobnih podataka. Posebne kategorije osobnih podataka dodatno su određene i opisane. Preciznije su opisane postojeće osjetljive kategorije osobnih podataka u zdravstvenoj djelatnosti čime su ojačana prava ispitanika kao i obaveze voditelja zbirki osobnih podataka prema inspekcijskim nadzorima. Na taj način Opća uredba o zaštiti podataka postaje jedinstven skup pravila koji se temelji na zajedničkom pristupu EU-a zaštiti osobnih podataka te se izravno primjenjuje u svim državama članicama.

Uredba dodatno postrožuje i aktivnosti prilikom obrade posebnih kategorija podataka u području “e-zdravstva“ te su problemi s kojima se praktičari svakodnevno susreću tijekom primjene zahtjeva Uredbe u svakodnevnom radu bili glavni motivatori za pisanje ovog rada. Glavni cilj koji se želi postići je ukazati na važnost podizanja svijesti o zaštiti posebnih kategorija osobnih podataka, zdravstvenih podataka, te podizanja organizacijskih i tehničkih mjera zaštite osobnih podatka na višu razinu kao i problemi koji proizlaze kroz uspostavu organizacijskih i tehničkih mjera.

Ključne riječi: Uredba, pojmovi Uredbe, prednosti i nedostaci Uredbe, pozitivni i negativni učinci implementacije Uredbe, zdravstveni sustav

Summary

Regulation (EU) 2016/679 of the European Parliament and of the Council represents a major step forward in the field of personal data protection and information security as it arose as a result of insufficiently effective previous national legislation in the field of virtual environment and protection of EU citizens' rights. The development of human activities in the digital world entails the accelerated development of information and communication technologies, while at the same time creating new challenges and threats to privacy and personal data protection. Data processing, in particular the processing of specific categories of personal data such as health data, new IT tools and the digital market, has developed a need to increase the protection of privacy of new digital products and services that process these categories of personal dana as justified.

The GDPR should ensure uniform treatment in the process of personal data processing. Special categories of personal data are additionally specified and defined. The existing sensitive categories of personal data in the healthcare sector are described in more detail, which strengthens the rights of subjects as well as the obligations of personal data collection managers towards inspections. In this way, the General Data Protection Regulation becomes a single set of rules based on a common EU approach to personal data protection and directly applicable in all Member States.

The Regulation further tightens the activities for processing special categories of data in the field of "e-health" and the problems that practitioners encounter during the application of the Regulation in everyday work were the main motivators for writing this paper. , and the goal was to show positive and negative effects of this Regulation in everyday health system practice. The main goal was to point out the importance of raising awareness about the protection of special categories of personal data, health data, and raising organizational and technical measures for personal data protection to a higher level as well as problems arising from the establishment of organizational and technical measures.

Key words: The General Data Protection Regulation, Regulation terms, advantages and disadvantages of the Regulation, positive and negative effects the Regulation, health care system

Zahvale

Zahvaljujem se mentoru prof. dr. sc. Stjepanu Oreškoviću, na pozitivnom stavu te podršci u prepoznavanju važnosti obrađene teme i lijepim riječima na račun originalnosti.

Curriculum Vitae (CV)

dr.sc. Petra Nola Fuchs, dr.med.dent., spec.
Državljanstvo: hrvatsko
Datum rođenja: 11.06.1981.
Spol: Žensko
Telefon: (+385) 996180000
E-adresa: pnolafuchs@spz.hr
Adresa: Augusta Šenoe 11, 10000 Zagreb (Hrvatska)

RADNO ISKUSTVO

Ravnateljica Stomatološke poliklinike Zagreb
Stomatološka poliklinika Zagreb [18.09.2020. - trenutačno]
Ravnateljica Stomatološke poliklinike Zagreb
Stomatološka poliklinika Zagreb [28.03.2017. – 18.09.2020.]
Mjesto: Zagreb, Perkovčeva 3
Zemlja: Hrvatska

Specijalist Oralne kirurgije
Stomatološka poliklinika Zagreb [2012. – 2017.]
Mjesto: Zagreb, Perkovčeva 3
Zemlja: Hrvatska

Specijalizantica iz Oralne kirurgije
Stomatološka poliklinika Zagreb [2008. – 2012.]
Mjesto: Zagreb, Perkovčeva 3
Zemlja: Hrvatska

Pripravnik - volonter
Stomatološka poliklinika Zagreb [2006. – 2007.]
Mjesto: Zagreb, Perkovčeva 3
Zemlja: Hrvatska

OBRAZOVANJE I OSPOSOBLJAVANJE

Menadžerica u zdravstvenim ustanovama
Effectus studij financije i pravo - Visoko učilište Zagreb [14.06.2018.]
Adresa: Trg Johna Kennedyja 2,10000 Zagreb

Položen specijalistički ispit iz oralne kirurgije
Republika Hrvatska, Ministarstvo zdravlja (02.07.2012.)

Izbor u znanstveno zvanje "Znanstveni suradnik"
Stomatološki fakultet Sveučilišta u Zagrebu [2011.]
Adresa: Gundulićeva 5, 10000 Zagreb

Donesena odluka o imenovanju stručnog povjerenstva za utvrđivanje uvjeta pristupnice za izbor u znanstveno zvanje „Viši znanstveni suradnik“ [2022.]

Stomatološki fakultet Sveučilišta u Zagrebu [2011.]
Adresa: Gundulićeva 5, 10000 Zagreb

Doktor znanosti
Stomatološki fakultet Sveučilišta u Zagrebu [2007. – 2011.]
Adresa: Gundulićeva 5, 10000 Zagreb
Područja obrazovanja: Zdravstvo i socijalna skrb : Stomatologija
„Detekcija humanog papiloma virusa 16 i Epstein-Barrovog virusa u oboljelih od planocelularnog karcinoma usne šupljine"

Položen državni i stručni ispit [12/10/2006.]

Doktor stomatologije
Stomatološki fakultet Sveučilišta u Zagrebu [1999. – 2005.]
Adresa: Gundulićeva 5, 10000 Zagreb

PROJEKTI

Voditelj Projekta "Pokretni geronto - stomatološki specijalistički timovi" Stomatološke poliklinike Zagreb [2018. – Trenutačno]

Voditelj "Programa osoba s teškoćama u razvoju" Stomatološke poliklinike Zagreb

[2017. – Trenutačno]

Voditelj "Programa prevencije karijesa djece predškolske i školske dobi u Gradu Zagrebu" Stomatološke poliklinike Zagreb

[2017. – Trenutačno]

ZNANSTVENI RADOVI

Oral Health Knowledge, Attitude, and Behavior of Nursing and Technical Students in Croatia Tomislav Cabov1, Ksenija Eljuga2, Petra Nola Fuchs1, Maja Kinkela Devcic1, Jelena Prpic3, Zoran Kovac4, Zrinka Puharic2, Irena Glazar3, Mirna Zulec2;

Published online: 2021-08-24

Odontomas: Pediatric case report and review of the literature

Tomislav Ćabov1, Petra Nola Fuchs1,3, Ana Zulijani2 , Lucija Ćabov Ercegović3 and Srđan Marelić; Acta Clin Croat 2021; 60:146-152

3-D stress analysis in first maxilliary premolar

Borčić J., Antonić R., Urek M., Petričević N., Nola-Fuchs P., Čatić A., Smojver I.; Coll Antropol 2007; 31: 1025-9

The prevalence of human papillomavirus 16 and Epstein-barr virus in patients with oral squamous cell carcinoma

P.Nola-Fuchs, V.Vučićević Boras, V.Plečko, S.Pleština, A. Milenović, M.Sušić i V.Brailo;

Acta Clin Croat 2012; 51:609-614

Salivary analytes in patients with oral squamous cell carcinoma
Nola-Fuchs P., Rogić D., Vidović-Juras D., Sušić M., Milenović A., Brailo V., Vučićević Boras V.;
Coll Antopol 2011; 36:1

Pain Relive after Impacted Wisdom Teeth Extraction Dependent on the Drug Therapy
Petra Nola-Fuchs, Edin Selimović, Lejla Ibrahimagić-Šeper, Nikola Petričević;
Coll.Antropol. 35(2011) 1:133-136

Congruency and divergency of calcium in the biological matrice of the human hair whit other osteotrophic and non-osteotrophic members of the multielement profile
Prejac J., Čelebić A., Stipetić-Ovčaićek J., Poljak-Guberina R., Nola-Fuchs P., Viktorovich Skalny A., Germadievna Skalnaya M., Momčilović B.
13th International Meeting on Trace Elements in Man and Animales, Pucon-Chile, November 9-13th, Book of abstracts, 2008.

Selection of the appropriate artificial frontal teeth
Ibrahimagić-Šeper L., Petričević N., Nola-Fuchs P., Stipetić J., 11th Congress of the BaSS, Sarajevo, May 2006.

Use of digital photographs for artificial tooth selection
Celebić A., Stipetić J., Nola P., Petričević N., Papić M.; Coll Antropol 2004; 28: 857-63

Artificial Tooth selection: could digital photographs be helpful?
Stipetić J., Čelebić J., Nola P., Petričević N., Knezović-Zlatarić D., Baučić I., Baučić-Božić M.,
29th Annual Conference of the European Prosthodontic Association
Prot. Stom. Poznan, Poljska 2005; Vol LV, 117.

FDI World Dental Congress
Montreal 2005 Arteficial teeth selection from digital photographs

Optimal place for tissue harvesting for free subepitelial graft
Baučić M., Stipetić J., Čelebić A., Knezović-Zlatarić D., Baučić I., Nola P. 28th Annual Conference of the European Prosthodontic Association
Izmir, Turkey 2004.

PREDAVANJA

"Sustav održivosti specijalizacija liječnika dentalne medicine"
[2018.]
121 Konferencija Udruge poslodavaca u zdravstvu Hrvatske
Opatija

"Izazovi i mogućnosti Stomatološke poliklinike Zagreb na otvorenom tržištu"
[2018.]
120 Konferencija Udruge poslodavaca u zdravstvu Hrvatske
Opatija

"Alveotomija impaktiranih umnjaka - korist ili šteta za pacijenta"
[02.2015.]
Stomatologija danas
Split

"All on 4 - funkcija i estetika u 24 sata"
[09.2014.]
Međunarodni kongres: Ljepota i estetika
Solaris, Šibenik

"All on 4 - funkcija i estetika u 24 sata"
[10.2014.]

7. Kongres novih tehnologija: Estetska stomatologija - umjetnost i znanost Skoplje, Makedonija

MREŽE I ČLANSTVA

Članstva:

- Udruga poslodavca
- Hrvatski liječničku zbor
- Stomatološka sekcija Zbora Liječnika
- Hrvatsko antropološko društvo
- Hrvatsko društvo za maksilofacijalnu, plastičnu i rekonstrukcijsku kirurgiju glave i vrata
- Hrvatsko Društvo za Dentalnu implantologiju

Imenovana dopredsjednicom Udruge poslodavaca u zdravstvu
[2022. – Trenutačno]

Imenovana članom u Uređivačkom odboru glasila Stomatološke komore Federacije Bosne i Hercegovine
[2014. – Trenutačno]

Imenovana članom "Savjeta za zdravlje"
[2021. – Trenutačno]
Odluka Gradske skupštine Grada Zagreba

Imenovana članom Uređivačkog odbora "Vjesnik"
[2020. – Trenutačno]

Imenovana predsjednicom "Sekcije za gerontostomatologiju"
[2019. – Trenutačno]

Imenovana članom Stručnog povjerenstva u području stomatologije u svrhu provjera operacija unutar Operativnog programa "Konkurentnost i kohezija 2014. -2020."
[2019. – 2020.]
Odluka Ministarstva zdravstva

Imenovana članom Upravnog vijeća KBC "Sestre milosrdnice"
[2018. – Trenutačno]

Imenovana članom Znanstvenog savjeta Komore
[2018. – Trenutačno]
Odluka Hrvatske komore dentalne medicine

Imenovana članom Predsjedništva Udruge poslodavaca u zdravstvu
[2018. – 2022.]

Imenovana članom Povjerenstva za specijalističku zaštitu dentalne medicine
[2017. – Trenutačno]

Imenovana članom "Savjeta za zdravlje"
[2017. – 2021.]
Odluka Gradske skupštine Grada Zagreba

Imenovana članom uredništva: http://www.mojstomatolog.hr/
[2013.]

NADZOR

Odlukom Povjerenstva za obavljanje stručnih nadzora Hrvatske komore dentalne medicine, uvrštena na listu doktora dentalne medicine koji provode stručni nadzor za područno sjedište Zagreb
[2018. – Trenutačno]

POČASTI I NAGRADE

Rektorova nagrada za najbolji studentski rad
Stomatološki fakultet Sveučilišta u Zagrebu [2004.]
„Određivanje najpovoljnijeg mjesta za uzimanje sluzničkog autotransplantata u području tvrdog nepca i tubera“

NASTAVA

Održava nastavu za studente na Medicinskom fakultetu Sveučilišta u Rijeci

[2018. – Trenutačno]

Sveučilišni studij: "Dentalna medicina", predmet Oralna kirurgija

Hitna stanja u oralnoj kirurgiji

Udžbenici Sveučilišta u Zagrebu

[2018.]

ČLANCI U STRUČNIM ČASOPISIMA

Bol kao uzrok dolaska u ordinaciju

[2015.]

Smile (2/15)

Rekonstrukcija defekta u mandibuli presadkom kriste ilijake

[2014.]

Petra Nola Fuchs, Marin Jurlina, Vjesnik dentalne medicine (2/14)

Oralne komplikacije terapije tumora

[2014.]

Smile (5/14)

Što kada imam "proces" na zubu

[2014.]

Smile (8/14)

HPV kao uzročnik karcinoma

[2014.]

Smile (6/14)

Problemi sa žlijezdama slinovnicama

[2014.]

Smile (7/14)

Oporavak nakon oralno kirurškog zahvata

[2013.]

Smile broj 1 (3/13)

JEZIČNE VJEŠTINE

Materinski jezik: Hrvatski

Strani jezici: Engleski, Njemački i Talijanski

SLUŠANJE: C2

ČITANJE: C2

PISANJE: C2

GOVORNA PRODUKCIJA: C2

GOVORNA INTERAKCIJA: C2

OBITELJ

Udana, majka troje djece

VOZAČKA DOZVOLA

Vozačka dozvola: B