P/219900

REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA

KLASA: UP/I-034-01/24-01/23
URBROJ: 567-04-02/03-24-1
Zagreb, 21.8.2024.

Agencija za zaštitu osobnih podataka (OIB: 28454963989), na temelju članaka 57. stavka 1., 58. stavka 1. i 2. točke (i) i 83. Uredbe (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) Službeni list Europske unije L119 i članaka 6., 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka ("Narodne novine" br. 42/18), u postupku pokrenutom po službenoj dužnosti protiv Specijalne bolnice Medico iz Rijeke, Agatićeva 8, OIB: 57951842896, zastupane po odvjetničkom uredu Vukić i partneri iz Rijeke, Nikole Tesle 9, OIB: 01394705384:, donosi sljedeće:

R J E Š E NJ E

1. Utvrđuje se da Specijalna bolnica Medico iz Rijeke, Agatićeva 8 kao voditelj obrade osobnih podataka nije na odgovarajući način propisala rokove čuvanja osobnih podataka iz snimki telefonskih razgovora, a što je protivno odredbi članka 5. stavka 1. točke (e) Opće uredbe o zaštiti podataka.

2. Utvrđuje se da Specijalna bolnica Medico iz Rijeke, Agatićeva 8 kao voditelj obrade osobnih podataka obrađuje osobne podatke ispitanika putem snimanja telefonskih razgovora putem pozivnog centra dostupnog na broju 072 100 100 bez pravne osnove iz članka 6. stavka 1. Opće uredbe o zaštiti podataka odnosno kako ista u svezi s člankom 5. stavka 2. Opće uredbe o zaštiti podataka nije dokazala pravnu osnovu za snimanje telefonskih razgovora.

3. Utvrđuje se da Specijalna bolnica Medico iz Rijeke, Agatićeva 8 kao voditelj obrade osobnih podataka prilikom uspostave poziva na pozivnom centru dostupnom putem broja 072 100 100 nije informirala ispitanike o obradi osobnih podataka koristeći jasan i jednostavan jezik, a što je protivno odredbi članka 12. stavka 1. Opće uredbe o zaštiti podataka te da nije pružila ispitanicima sve potrebne informacije o prikupljanju njihovih osobnih podataka putem snimanja telefonskih razgovora na

način propisan sukladno odredbi članka 13. stavka 1. točke (c) i stavka 2. točke (a) i (b) Opće uredbe o zaštiti podataka.

4. Utvrđuje se da Specijalna bolnica Medico iz Rijeke, Agatićeva 8 kao voditelj obrade osobnih podataka nije sklopila ugovor o obradi osobnih podataka s društvom Veridian Healthstream d.o.o. iz Zagreba, Ulica majstora Radonje 14 kao izvršiteljem obrade osobnih podataka, a što je protivno odredbi članka 28. stavka 3. Opće uredbe o zaštiti podataka.

5. Utvrđuje se da Specijalna bolnica Medico iz Rijeke, Agatićeva 8 kao voditelj obrade osobnih podataka nije implementirala odgovarajuće tehničke mjere zaštite informacijskog radiološkog sustava u pogledu slikovnih datoteka (osobnih podataka) u odnosu na izradu sigurnosnih kopija osobnih podataka, a što je protivno odredbi članka 32. stavka 1. točke (b) Opće uredbe o zaštiti podataka.

6. Utvrđuje se da Specijalna bolnica Medico iz Rijeke, Agatićeva 8 kao voditelj obrade osobnih podataka nije informirala Agenciju o sigurnosnom incidentu gubitka osobnih podataka ispitanika u pogledu slikovnih datoteka (osobnih podataka) iz radiološkog informacijskog sustava iz srpnja 2019. godine u roku od 72 sata od trenutka saznanja za incident, a što je protivno odredbi članka 33. stavka 1. Opće uredbe o zaštiti podataka.

7. Utvrđuje se da Specijalna bolnica Medico iz Rijeke, Agatićeva 8 kao voditelj obrade osobnih podataka nije uključila službenicu za zaštitu podataka u pitanja vezana uz izradu/doradu politike privatnosti te u vezi snimanja telefonskih razgovora i propisivanja rokova čuvanja snimki telefonskih razgovora, a što je protivno odredbi članka 38. stavka 1. Opće uredbe o zaštiti podataka.

8. Uslijed utvrđenih povreda Opće uredbe o zaštiti podataka iz točaka 1. – 7. izreke ovog Rješenja, Specijalnoj bolnici Medico iz Rijeke, Agatićeva 8 kao voditelju obrade osobnih podataka izriče se upravno novčana kazna u iznosu od

190.000,00 Eura (slovima: stotinudevedesettisuća eura)

Specijalna bolnica Medico iz Rijeke, Agatićeva 8 dužna je platiti izrečenu upravnu novčanu kaznu u korist državnog proračuna u roku od 15 dana od dana pravomoćnosti ovog rješenja u korist računa broj:
HR1210010051863000160, model HR64 i poziv na broj odobrenja 6092-25860-57951842896 s naznakom – "upravne novčane kazne koje izriče AZOP".

9. Ukoliko Specijalna bolnica Medico iz Rijeke, Agatićeva 8, u roku od 15 dana od pravomoćnosti ovog rješenja ne plati izrečenu upravnu novčanu kaznu, Agencija će sukladno članku 46. stavku 2. Zakona o provedbi Opće uredbe o zaštiti podataka

obavijestiti Područni ured Porezne uprave Ministarstva financija na čijem je području sjedište navedenog društva radi naplate upravne novčane kazne prisilnim putem prema propisima o prisilnoj naplati poreza.

10. Specijalna bolnica Medico iz Rijeke, Agatićeva 8 je dužna u roku od 15 dana od izvršene uplate dostaviti dokaz o uplati na uvid ovoj Agenciji.

O b r a z l o ž e n j e

I. UTVRĐENJE POVREDE PRAVA NA ZAŠTITU OSOBNIH PODATAKA

Agencija za zaštitu osobnih podataka zaprimila je više zahtjeva za utvrđivanje povrede prava na zaštitu osobnih podataka zbog nedostavljanja kopija osobnih podataka od strane Specijalne bolnice Medico iz Rijeke, Agatićeva 8 kao voditelja obrade osobnih podataka (dalje u tekstu: Specijalna bolnica), a do čega je došlo zbog gubitka osobnih podataka zdravstvene kategorije od strane Specijalne bolnice Medico u srpnju 2019. godine. Budući da je nakon zaprimanja zahtjeva u okviru upravnog postupka Agencija došla do saznanja odnosno sumnje da je Specijalna bolnica Medico povrijedila veći broj odredbi Opće uredbe o zaštiti podataka u odnosu na veći broj ispitanika, Agencija je pokrenula postupak po službenoj dužnosti.

Slijedom gore iznesenog, Agencija je dopisom od dana 22. studenog 2023. godine (preslika prileži spisu predmeta) zatražila očitovanje Specijalne bolnice u pogledu, između ostalog, točnog trenutka saznanja za sigurnosni incident gdje su u srpnju 2019. godine izgubljeni podaci nekolicine ispitanika u pogledu slika njihovih radioloških nalaza te razloga iz kojega takav inicident nije prijavljen Agenciji temeljem odredbi članka 33. stavka 1. Opće uredbe o zaštiti podataka. Budući da zatraženo očitovanje nije zaprimljeno do 08. prosinca 2023. godine Agencija je dana 08. prosinca 2023. godine na adresu elektroničke pošte x uputila požurnicu.

Na takvo traženje Agencije Specijalna bolnica je putem odvjetničkog ureda Vukić i partneri iz Rijeke, Nikole Tesle 9 dopisom od 07. prosinca 2023. godine uputila svoje očitovanje Agenciji, ali u kojemu se ista očitovala kako uslijed proteka vremena ne zna za ukupan broj ispitanika čiji podaci su uistinu bespovratno izgubljeni te kako iz istog razloga ne znaju za točan trenutak saznanja za sigurnosni incident dok se u odnosu na razlog ne prijavljivanja istog Agenciji Specijalna bolnica nije očitovala.

Nadalje, dopisom od 08. prosinca 2023. godine Agencija je zatražila očitovanje Specijalnu bolnicu u odnosu na razloge iz kojih politika privatnosti dostupna putem URL poveznice https://www.medico.hr/o-nama/pravila-zastite-osobnih-podataka/ ne sadrži podatke o snimanju telefonskih razgovora te prateće elemente iz članka 13. Opće uredbe o zaštiti podataka koji se odnose na snimanje telefonskih razgovora (uključivo svrhu, pravnu osnovu, kategoriju podataka, rokove čuvanja, mogućnost ulaganja prigovora na snimanje razgovora), zatim

detaljno očitovanje odnosno na svrhu i pravnu osnovu snimanja telefonskih razgovora te razlogu korištenja formulacije : „razgovor može biti sniman“, a u kontekstu korištenja jasnog i jednostavnog jezika iz članka 12. stavka 1. Opće uredbe o zaštiti podataka.

Agencija je dopisom od 08. prosinca 2023. godine na traženje Specijalne bolnice produžila rok za očitovanje do zaključno 18. prosinca 2023. godine uz potrebu očitovanja vezanog uz poštivanje članka 33. stavka 1. Opće uredbe o zaštiti podataka te dostavu ugovora o obradi osobnih podataka s društvom Veridian Healthstream iz Zagreba, Ulica majstora Radonje 14 (dalje u tekstu: Veridian) vezanog uz održavanje IT sustava od strane Veridiana kao izvršitelja obrade po članku 28. stavku 3. Opće uredbe o zaštiti podataka.

Na takvo traženje Agencije Specijalna bolnica je dopisom od 20. prosinca 2023. godine zamolila Agenciju za opetovano produženje roka za dostavu očitovanja budući da je dopis Agencije zaprimila tek 19. prosinca 2023. godine te se Specijalna bolnica nije niti naknadno očitovala na gore zatražene okolnosti.

U svrhu točnog i potpunog utvrđivanja činjeničnog stanja Agencija je dana 28. veljače 2024. godine provela izravno nadzorno postupanje u društvu Veridian, a o čemu je sastavljen i Zapisnik o provedenom nadzoru od 28. veljače 2024. godine (KLASA: 044-01/24-01/1; URBROJ: 567-04-01/01-24-9). U tijeku nadzora u bitnom je utvrđeno kako su lipnju 2018. godine započeli sa pregovorima u pogledu poslovne suradnje vezane uz implementaciju novog Radiološkog informacijskog sustava te sustava za arhiviranje slika radioloških nalaza (RIS/PACS), kao i održavanje sustava. Ugovor o poslovnoj suradnji potpisan je 26. studenog 2018. godine, dok je predmetni sustav implementiran u bolnicu 01. ožujka 2019. godine. Direktor Veridiana je naveo kako je u bolnici prije toga bilo implementirano za istu uslugu programsko rješenje društva Y d.o.o. U odnosu na posebno postavljeno pitanje ovlaštenog službenika Agencije da li je osim ugovora o poslovnoj suradnji možebitno sklopljen još kakav ugovor ili aneks ugovora odnosan isključivo na obradu osobnih podataka direktor je izjavio kako osim nekoliko članaka iz ugovora o poslovnoj suradnji ne postoji zaseban ugovor odnosan na obradu osobnih podataka. Na daljnje pitanje ovlaštenog službenika Agencije da pojasni odnos sa Specijalnom bolnicom u smislu voditelja/izvršitelja obrade direktor je izjavio kako su oni izvršitelji obrade za bolnicu u pogledu gore navedene usluge te je isti priložio presliku ugovora o poslovnoj suradnji sklopljenog sa Specijalnom bolnicom.

U nadzoru je isto tako utvrđeno kako je s obzirom da se u novi sustav nisu mogli importirati stari radiološki nalazi, Specijalna bolnica donijela odluku kako će za nalaze koji su rađeni do uvođenja novog sustava koristiti i dalje stari sustav, a za nove nalaze podatke iz novog sustava. Nadalje Veridian je također naveo kako su na radnim sastancima prije konačnog puštanja u rad njihovog sustava usmeno upozoravali predstavnike bolnice kako se radi o serveru starom između 10 i 15 godina te kako su na istom potrebni zahvati nadogradnje/obnavljanja kako bi ostao i dalje funkcionalan.

Direktor Veridiana je također izjavio kako su došli do spoznaje kako je u 7. mjesecu 2019. došlo do kvara na serveru na kojem su bili pohranjeni podaci i programsko rješenje koje se

koristilo za radiološke nalaze prije implementacije njihovog rješenja te da bolnica od tada nije mogla pristupati tim podacima. Djelatnik društva Veridian je u duhu dobre poslovne suradnje, a izvan ugovorih usluga, pokušao osposobiti navedeni server međutim u tome nije uspio te su bolnici dali usmene upute što bi trebali napraviti kako bi ga osposobili međutim nemaju povratne informacije da li je do toga i došlo.

Na izravan upit ovlaštenih službenika Agencije da li je dogovoren poslovni/ugovorni odnos vezano za backup podataka iz sustava, direktor je isto tako naveo kako je u njihovom sustavu omogućen backup podataka samog sustava, ali oni nemaju obvezu to raditi već je to na Specijalnoj bolnici kao voditelju obrade da redovito radi backup podataka sustava. Nadalje na izravan upit ovlaštenih službenika Agencije ima li spoznaje da je Specijalna bolnica radila backup podataka iz starog sustava, direktor je izjavio kako nema informacija o tome te da bi o tome trebalo eventualno vidjeti sa društvom Y d.o.o. koje je implementiralo i održavalo stari sustav.

Nakon toga je Agencija dana 29. veljače 2024. godine provela izravne nadzorne aktivnosti kod Specijalne bolnice, a o čemu je sastavljen Zapisnik o provedenom nadzoru od 07. ožujka 2024. godine (KLASA: 044-01/24-01/1; URBROJ: 567-04-01/01-24-12). U nadzoru je u bitnom utvrđeno kako društvo Veridian pruža usluge održavanja radiološkog informacijskog sustava te kako je za predmetne usluge sklopljen ugovor o poslovnoj suradnji koji je u tijeku nadzora priložen te isti čini sastavni dio spisa predmeta. Na posebno postavljen upit ovlaštenog službenika Agencije da li osim priloženog ugovora postoje još neki ugovori s društvom Veridian, a osobito ugovor o obradi osobnih podataka službenica za zaštitu podataka Specijalne bolnice je izjavila kako ne postoji ugovor o obradi osobnih podataka te kako je navedeno društvo u smislu Opće uredbe o zaštiti podataka izvršitelj obrade osobnih podataka Specijalne bolnice.

Na postavljeno pitanje ovlaštenog službenika Agencije da pojasni gubitak osobnih podataka iz informacijskog sustava vezanog uz radiološke usluge bolnice u srpnju 2019. godine te s tim u svezi podnošenje zahtjeva ispitanika za pristupom njihovim osobnim podacima temeljem članka 15. Opće uredbe o zaštiti podataka, službenica za zaštitu podataka je pojasnila kako su zaprimili između 2 do 5 takvih zahtjeva ispitanika, a kojima nisu mogli udovoljiti iz razloga što su osobni podaci izgubljeni u srpnju 2019. godine nakon informatičkog incidenta o kojem ne zna detalje. Nadalje, a na posebno postavljeno pitanje ovlaštenog službenika Agencije od kolikog ukupnog broja ispitanika su nestali osobni podaci iz radiološkog sustava u srpnju 2019. godine ista je izjavila kako ne zna koliki je broj ispitanika čiji podaci su izgubljeni te kako ne zna kakva je bila procedura oko pronalaska gubitaka i da li je provođena procjena rizika u odnosu na prava i slobode ispitanika kod gubitka njihovih osobnih podataka. Na upit u kojem trenutku su saznali za gubitak osobnih podataka ista je izjavila kako su saznali tek nakon obraćanja ispitanika za pristupom podacima, a koju korespondenciju će naknadno dostaviti Agenciji.

Informatičar Specijalne bolnice je u nadzoru izjavio kako društvo Veridian može radiološkom informacijskom sustavu bolnice pristupiti na dva načina tj. da imaju mogućnost fizičkog

pristupa radiološkom informacijskom sustavu bolnice unutar iste te udaljenim pristupom putem VPN tunela kreiranog na Fortigate vatrozidu bolnice. Isto tako je izjavio kako je informacijski sustav bolnice od malicioznih sadržaja zaštićen putem antivirusnog programa X.

Na posebno postavljen upit ovlaštenog službenika Agencije da li postoji backup radiološkog informacijskog sustava informatičar je nakon što je u tijeku nadzora stupio u kontakt s društvom Veridian (preslika elektroničke korespondencije je priložena u tijeku nadzora) naveo kako backup sustava postoji, te kako se iz sustava radi dnevni backup RIS i PACS baza podataka i da se iste nakon toga eksportiraju na dediciranu lokaciju unutar bolničke mreže, dok se backup slikovne arhive iz radiološkog informacijskog sustava ne radi budući da je dokumentacija opsežna i sastoji se od velike količine podataka, a čiji backup bi iziskivao veće resurse odnosno dodatna ulaganja u informacijski sustav bolnice.

Na posebno postavljeno pitanje ovlaštenog službenika Agencije u koju svrhu i temeljem koje pravne osnove se snimaju telefonski razgovori s ispitanicima putem call centra Specijalne bolnice Medico, a koji je dostupan putem telefonskog broja 072 100 700 ista je izjavila kako se razgovori snimaju u svrhu unaprjeđenja usluga te dokazivanja sadržaja razgovora s pacijentima koji često puta imaju prigovore u pogledu ugovorenih medicinskih usluga. U odnosu na pravnu osnovu iz članka 6. stavka 1. Opće uredbe o zaštiti podataka temeljem kojih se snimaju telefonski razgovori, odnosno pojašnjenje koja od šest tamo propisanih pravnih osnova se koristi za obradu osobnih podataka ista je izjavila kako ne zna koja je pravna osnova za obradu osobnih podataka te je molila za pojašnjenje ovlaštenog službenika Agencije u pogledu pravnih osnova koje postoje za obradu osobnih podataka. Također je pojasnila kako u pogledu snimanja telefonskih razgovora nije rađena procjena rizika niti bilo kakav test razmjernosti kojim bi se procijenio utjecaj na prava ispitanika.

Nastavno na pitanje ovlaštenog službenika Agencije da pojasni iz kojeg razloga se u tijeku telefonskog razgovora s call centrom Specijalne bolnice Medico koristi jezična formulacija: „ovaj razgovor može biti sniman“ umjesto „ovaj razgovor se snima“ u korelaciji s odredbom članka 12. Opće uredbe o zaštiti podataka u pogledu korištenja jasnog i jednostavnog jezika službenica za zaštitu podataka je navela kako nije sigurna za razlog te kako pretpostavlja kako se navedena formulacija koristi zbog kratkoće vremena snimanja razgovora. Na upit službenika na koji način su ispitanici informirani o obradi osobnih podataka o snimanju telefonskih razgovora ista navodi kako su o tome informirani samo na početku telefonskog razgovora putem call centra. Na posebno postavljen upit od kojeg datuma se koristi funkcija snimanja telefonskih razgovora te koliki su rokovi čuvanja razgovora i kojim aktima su propisani rokovi čuvanja, ista je izjavila kako ne zna od kada se snimaju telefonski razgovori te koliki je broj ispitanika čiji razgovori su snimljeni te koji su rokovi čuvanja snimki telefonskih razgovora i kako ne zna za postojanje internog akta kojim su propisani rokovi čuvanja snimki telefonskih razgovora. Na upit ovlaštenog službenika Agencije da li je kao službenica za zaštitu podataka bila aktivno uključena u razgovore oko snimanja telefonskih razgovora te propisivanja rokova čuvanja istih i možebitno informiranja ispitanika, ista je izjavila kako nije bila uključena u navedeno.

Na upit da li je kao službenica za zaštitu podataka bila uključena u razgovore oko politike privatnosti te da li postoji politika privatnosti bolnice ista je izjavila kako postoji politika privatnosti te kako će istu naknadno dostaviti Agenciji i kako nije bila uključena u razgovore oko izrade ili dorade politike privatnosti.

Informatičar je u pogledu snimanja telefonskih razgovora dodatno objasnio kako pristup snimkama imaju zaposlenici Call centra te kako po njegovim saznanjima uposlenici Call centra mogu pristupiti snimci ne starijoj od godinu dana i ista se može pronaći putem aplikativnog rješenja koje pruža društvo XY unutar filtera, dok je pronalaženje i starije snimke možda moguće zaposlenicima društva XY. U tijeku nadzora informatičar je ovlaštenicima službenicima Agencije predao USB prijenosnu memoriju na kojoj su presnimljene dvije snimke razgovora i to od 02. siječnja 2023. te 29. veljače 2024, te isto prileži spisu predmeta.

Budući da u tijeku nadzora ovlaštenim službenicima Agencije nije predana cjelokupna relevantna dokumentacija odnosna na obradu osobnih podataka ispitanika, Agencija je Zapisnikom od 07. ožujka 2024. godine obvezala Specijalnu bolnicu na dostavu, između ostalog, elektroničke korespondencije između bolnice te svih ispitanika koji su tražili pristup svojim osobnim podacima temeljem članka 15. Opće uredbe o zaštiti podataka, a kojima nije udovoljeno iz razloga gubitka osobnih podataka nakon srpnja 2019. godine; ukupnog broja ispitanika čiji osobni podaci su izgubljeni u srpnju 2019. godine kada je došlo do promjena na informacijskom sustavu za korištenje radioloških usluga (PACS/RIX); relevantnog dokaza da li su o incidentu koji je nastao gubitkom osobnih podataka ispitanika u srpnju 2019. godine o tome obavijestili Agenciju za zaštitu osobnih podataka; ukupnog broj ispitanika čiji telefonski razgovori su snimljeni putem call centra dostupnog na broj 072 100 700 od uspostave funkcije snimanja razgovora, a koji su zabilježeni u aplikativnom rješenju bolnice unutar kojeg se bilježe telefonski razgovori; rokova čuvanja snimljenih telefonskih razgovora te kojim aktom su propisani rokovi čuvanja te politiku privatnosti bolnice.

Dana 01. ožujka 2024. godine ovlašteni službenik Agencije je pozivom na telefonski broj 072 100 100 oko 09:20 sati predmetnog dana utvrdio kako se na početku razgovora s pozivnim centrom prije nego li se stupi u kontakt s agentom koji radi na pozivnom centru ispitanicima navodi kako „ovaj razgovor može biti sniman u svrhu unaprjeđenja usluge“, a o čemu je snimljena audio datoteka telefonskog poziva te službena zabilješka koja prileži spisu predmeta.

Dana 19. ožujka 2024. godine Specijalna bolnica je dostavila Agenciji svoje očitovanje odnosno dostavila je dokumentaciju i informacije zatražene Zapisnikom o provedenom nadzoru od 07. ožujka 2024. godine. Ista je u bitnom navela kako je došlo do nepovratnog gubitka osobnih podataka X, X i X te kako se ne mogu detaljnije izjasniti o uzrocima gubitka osobnih podataka. U pogledu ostalih mogućih ispitanika kojima su možebitno izgubljeni osobni podaci Specijalna bolnica je navela kako se uslijed proteka vremena ne može o tome izjasniti. U pogledu snimki telefonskih razgovora u bitnom je navedeno kako je najstarija snimka u aplikaciji od 19. travnja 2021. godine, dok se snimkama u periodu od 22. travnja 2016. do 17. travnja 2021. godine može pristupiti putem servera te kako je na serveru snimljeno ukupno 617 333 razgovora, dok se u aplikaciji može pronaći ukupno 435 909 razgovora s ispitanicima. Razgovori mogu biti

snimljeni u svrhu unapređenja usluge te kako Specijalna bolnica ima u planu čuvati snimke najmanje 10 godina sukladno Zakonu o liječništvu, budući da se na istima mogu pronaći zdravstveni podaci. U privitku očitovanja Specijalna bolnica je dostavila presliku politike privatnosti kao i u bitnom presliku elektroničke korespondencije između Specijalne bolnice i X, X i X odnosnu na ostvarivanje prava na pristup osobnim podacima.

Nadalje, Agencija je dopisom od 26. lipnja 2024. godine zatražila dodatno očitovanje Specijalnu bolnicu u pogledu detaljnog očitovanja o tome na koji način se vodila evidencija pacijenata čiji osobni podaci su bili dio informacijskog radiološkog sustava koji je nepovratno izgubljen, odnosno čije radiološke slike su bile pohranjene unutar takvog sustava koji je promijenjen 2019. godine uz dostavu očitovanja o tome da li su osim u predmetnom sustavu podaci bili pohranjeni na nekom drugom mjestu ili mediju te ako jesu na kojemu i koliko ispitanika se nalazilo na istom. U svezi s netom iznesenim također je zatraženo da se Specijalna bolnica dodatno očituje o ukupnom broju ispitanika čiji osobni podaci se u pogledu slikovne arhive trenutno nalaze pohranjeni u radiološkom informacijskom sustavu bolnice.

Isto tako, a u svrhu detaljne provjere financijskog stanja Specijalne bolnice Medico Agencija je dopisom od 26. lipnja 2024. godine zatražila od Financijske agencije (dalje u tekstu: FINA) dostavu godišnjeg financijskog izvješća za 2023. godinu za Specijalnu bolnicu te je isto zaprimljeno dana 09. srpnja 2024. godine te prileži spisu predmeta.

Nadalje, Agencija je dana 03. srpnja 2024. godine zatražila dostavu dodatnih informacija od društva Veridian, a osobito u pogledu informacije o načinu na koji je društvo Veridian došlo do spoznaje da je došlo do kvara na serveru Specijalne bolnice i gubitka podataka te kada su saznali za isto te na koji način da je došlo do gubitka podataka iz radiološkog informacijskog sustava Specijalne bolnice uz dostavu relevantnih dokaza o svemu zatraženom.

Dana 04. srpnja 2024. godine Agencija je zaprimila zatražene informacije od društva Veridian, koje je u bitnom navelo kako im Specijalna bolnica nije dostavila povijesne radiološke nalaze u ugovorom definiranom formatu za import u novi radiološki informacijski sustav koji su oni isporučili te kako samim time društvo Veridian nije moglo importirati povijesne radiološke nalaze niti ih je moglo izgubiti. Navedeno je i kako su za kvar servera Specijalne bolnice saznali 23. srpnja 2019. oko podneva temeljem telefonskog poziva glavne inženjerke radiologije X prema kolegi X iz društva Veridian i o istome su obavijestili upravu. Zaključno navode kako društvo Veridian odbija odgovornost za gubitak osobnih podataka iz povijesnih radioloških nalaza. U privitku očitovanja društvo Veridian je u bitnom dostavilo elektroničku koresponenciju koja se odnosi na saznanje o sigurnosnom incidentu te ista prileži spisu predmeta. Dostavljena je elektronička pošta poslana s adrese X na adresu X dana 23. srpnja 2019. godine u 12:25h, a u kojoj X iz društva Veridian navodi kako je društvo Veridian u telefonskoj komunikaciji s glavnom inženjerkom radiologije saznalo kako od 23. srpnja 2019. godine u jutarnjim satima u sobi do reading room-a (radiologija) jedan od servera na kojem se nalazi RIS/PACS sustav Y društva počinje proizvoditi veliki količinu buke (ventilatori) te je server restartan od strane IM podrške. Nakon restarta, server im više nije dostupan. Na monitoru servera javila se greška u inicijalizaciji memorije.

Dana 08. srpnja 2024. godine Agencija je zaprimila dodatno očitovanje od Specijalne bolnice putem odvjetničkog društva Vukić i partneri, a u kojemu je u bitnom navedeno kako će se od društava koja im pružaju usluge održavanja hardverskog i softverskog dijela zatražiti detaljna očitovanja jesu li u predmetnom sustavu podaci bili pohranjeni na nekom drugom mjestu ili mediju te koliko ispitanika se na istima nalazilo, kao i očitovanja o ukupnom broju ispitanika čiji osobni podaci se u pogledu slikovne arhive trenutno nalaze pohranjeni u radiološkom sustavu Specijalne bolnice.

Također je navedeno kako Specijalna bolnica uredno vodi evidenciju svih svojih pacijenata pa tako i onih čiji su osobni podaci bili dio informacijskog sustava koji je nepovratno izgubljen te kako se moli Agencija za produljenje roka za dostavu svih zatraženih očitovanja budući da je rok od 3 dana kratak za dostavu svih zatraženih informacija.

Agencija je dana 10. srpnja 2024. godine odobrila Specijalnoj bolnici produženje gore zatraženog roka za očitovanje do kraja radnog dana 11. srpnja 2024. godine te isto nije zaprimljeno u zatraženom dodatnom roku.

Nastavno na navedeno, ističemo kako se od 25. svibnja 2018., u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, u području zaštite osobnih podataka izravno i obvezujuće primjenjuje 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) SL EU 119, a za čiju primjenu i provođenje na području Republike Hrvatske je nadležna Agencija za zaštitu osobnih podataka.

Članak 2. Opće uredbe o zaštiti podataka propisuje kako se ista primjenjuje na obradu osobnih podataka koja se u cijelosti obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.

Navedena Opća uredba o zaštiti podataka u članku 4. stavku 1. točki 1. propisuje da su osobni podaci svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, a pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. Točkom 7. definirano je kako je voditelj obrade fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice. Točkom 8. definirano je kako je izvršitelj obrade fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

Sukladno članku 5. stavku 1. Opće uredbe o zaštiti podataka osobni podaci moraju biti: a) zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika (načelo zakonitosti, poštenosti i transparentnosti); b) prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama (načelo ograničavanja svrhe); c) primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koju se obrađuju (načelo smanjenje količine podataka); d) točni i prema potrebi ažurni (načelo točnosti); e) čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju (načelo ograničenja pohrane); f) obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera (načelo cjelovitosti i povjerljivosti).

Članak 6. stavak 1. Opće uredbe o zaštiti podataka propisuje kako je obrada osobnih podataka zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećeg: a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha; b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora; c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade; d) obrada je nužna kako bi se zaštitili životno važni interesi ispitanika ili druge fizičke osobe; e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade; f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane.

Nadalje, člankom 12. stavkom 1. Opće uredbe o zaštiti podataka propisano je kako voditelj obrade poduzima odgovarajuće mjere kako bi se ispitaniku pružile sve informacije iz članaka 13. i 14. i sve komunikacije iz članaka od 15. do 22. i članka 34. u vezi s obradom u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, osobito za svaku informaciju koja je posebno namijenjena djetetu. Informacije se pružaju u pisanom obliku ili drugim sredstvima, među ostalim, ako je prikladno, elektroničkim putem. Ako to zatraži ispitanik, informacije se mogu pružiti usmenim putem, pod uvjetom da je drugim sredstvima utvrđen identitet ispitanika.

Člankom 13. Opće uredbe o zaštiti podataka propisano je kako je voditelj obrade u trenutku prikupljanja osobnih podataka obvezan ispitaniku pružiti informacije:

- o svom identitetu,
-o službeniku za zaštitu podataka (kontakt podaci službenika),
- upoznati sa svrhom i pravnom osnovom za obradu osobnih podataka,
-o primateljima ili kategorijama primatelja osobnih podataka,
-o prenošenju osobnih podataka trećoj zemlji ili međunarodnoj organizaciji (koje nisu članice EU),
-o legitimnom interesu, (stavak 1.)
-o vremenskom roku pohrane osobnih podataka te kriterijima kojima se utvrđuje razdoblje pohrane,

-o postojanju prava da se od voditelja obrade zatraži pristup osobnim podacima, ispravak, brisanje osobnih podataka ili ograničavanje obrade koja se na njega odnose, prava na ulaganje prigovora na obradu takvih podataka te na prenosivost njegovih podataka drugom voditelju obrade,
- o pravu da se u bilo kojem trenutku povuče privola, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena,
-o pravu na podnošenje prigovora nadzornom tijelu (Agenciji za zaštitu osobnih podataka)
-da li je pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže,
-o postojanju automatiziranog donošenja odluka, što uključuje izradu profila te smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za ispitanika. (stavak 2.)

Člankom 28. stavkom 1. Opće uredbe o zaštiti podataka propisano je kako se u slučaju kada se obrada provodi u ime voditelja obrade, voditelj obrade koristi jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz Opće uredbe o zaštiti podataka i da se njome osigurava zaštita prava ispitanika. Stavkom 2. propisano je kako izvršitelj obrade ne smije angažirati drugog izvršitelja obrade bez prethodnog posebnog ili općeg pisanog odobrenja voditelja obrade. U slučaju općeg pisanog odobrenja, izvršitelj obrade obavješćuje voditelja obrade o svim planiranim izmjenama u vezi s dodavanjem ili zamjenom drugih izvršitelja obrade kako bi time voditelju obrade omogućio da uloži prigovor na takve izmjene. Stavkom 3. definirano je kako se obrada koju provodi izvršitelj obrade uređuje ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice, koji izvršitelja obrade obvezuje prema voditelju obrade, a koji navodi predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade. U nastavku stavka taksativno su propisani obvezni sastojci takvog ugovora.

Članak 32. stavak 1. Opće uredbe o zaštiti podataka propisuje da uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi: (b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade i (d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, dok je stavkom 2. istoga članka propisano da se prilikom procjene odgovarajuće razine sigurnosti u obzir posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

Člankom 33. stavkom 1. Opće uredbe o zaštiti podataka propisano je kako u slučaju povrede osobnih podataka voditelj obrade bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72

sata nakon saznanja o toj povredi, izvješćuje nadzorno tijelo nadležno u skladu s člankom 55. o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje.

Zaključno, člankom 38. stavkom 1. Opće uredbe o zaštiti podataka propisano je kako voditelj obrade i izvršitelj obrade osiguravaju da je službenik za zaštitu podataka na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka.

U ovoj upravnoj stvari u bitnom je utvrđeno kako u pogledu propisivanja rokova čuvanja osobnih podataka dobivenih putem snimanja telefonskih razgovora Specijalna bolnica nije propisala internim aktima rokove čuvanja takvih osobnih podataka, a što je jasno utvrđeno u nadzoru od 29. veljače 2024. godine kada je prikupljena izjava kako Specijalna bolnica nije propisala rokove čuvanja takovih osobnih podataka. Nadalje, očitovanjem zaprimljenim u Agenciji dana 19. ožujka 2024. godine Specijalna bolnica je potvrdila kako takvi rokovi čuvanja nisu propisani internim aktima, već kako je trenutno u planu da se takve snimke i pripadajući osobni podaci ispitanika čuvaju najmanje 10 godina temeljem Zakona o liječništvu. Iz netom navedenog utvrđeno je kako Specijalna bolnica Medico nije vodila računa o svojoj pravnoj obvezi iz članka 5. stavka 1. točki (e) Opće uredbe o zaštiti podataka odnosno obvezi čuvanja podataka u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. U tom smislu Specijalna bolnica je jasno navela (a što proizlazi i iz dostavljenih audio snimki razgovora s ispitanicima) kako je svrha snimanja razgovora unapređenje pružanja usluge te je ista tada bila dužna propisati rokove čuvanja takovih osobnih podataka svojim internim aktom uzimajući u obzir najkraće vrijeme koje je nužno kako bi se očuvala odnosno unaprijedila kvaliteta pružanja usluga putem snimanja telefonskih razgovora, a što Specijalna bolnica uopće nije učinila. Nadalje, a uzgredno govoreći naknadno pozivanje Specijalne bolnice kako ima u planu snimke čuvati deset godina temeljem Zakona o liječništvu uopće nije primjenjivo u ovoj upravnoj stvari. Naime, člankom 23. stavkom 4. Zakona o liječništvu („Narodne novine“ br. 121/03 i 117/08) jasno je propisano kako se podaci o ambulantnom liječenju čuvaju deset godina nakon završenog liječenja te je već iz samog teksta pravne odredbe jasno kako ista nije primjenjiva u ovom slučaju te kako ne može predstavljati pravnu osnovu za čuvanje snimki deset godina budući da snimke telefonskih razgovora (od kojih sve zasigurno niti ne predstavljaju zdravstvene podatke) ne predstavljaju ambulanto liječenje bolesnika.

Isto tako je utvrđeno kako Specijalna bolnica Medico nije imala pravnu osnovu za snimanje telefonskih razgovora iz članka 6. stavka 1. Opće uredbe o zaštiti podataka odnosno kako istu nije dokazala u svezi s člankom 5. stavkom 2. Opće uredbe o zaštiti podataka. Naime, nadzorom od 29. veljače 2024. godine utvrđeno je kako Specijalna bolnica nije niti znala dati odgovor na pitanje koja je pravna osnova za snimanje telefonskih razgovora putem telefonskog broja 072 100 100 te je službenica za zaštitu podataka čak zamolila ovlaštenog službenika Agencije da joj navede koje pravne osnove za obradu osobnih podataka postoje u članku 6. stavku 1. Opće uredbe o zaštiti podataka te kako se uopće nije provodio primjerice test razmjernosti kojim bi se prije početka obrade osobnih podataka procijenio utjecaj takve invazivne metode obrade

osobnih podataka na prava i slobode ispitanika. Isto tako Specijalna bolnica u niti jednom dijelu upravnog postupka nije dokazala postojanje pravne osnove za takovu vrstu obrade osobnih podataka iako je u više navrata Agencija tražila upravno navedeno. Iz netom navedenog jasno je utvrđeno kako pravna osnova za snimanje telefonskih razgovora uopće nije postojala te kako je navedena obrada bila te i dalje jest protuzakonita.

Nadalje, u ovoj upravnoj stvari utvrđeno je kako se kod snimanja telefonskih razgovora upućenih na broj 072 100 100 (pozivni centar Specijalne bolnice) neposredno prije spajanja s agentom koji preuzima konkretni poziv putem automatske sekretarice ispitanicima uputi sljedeća jezična formulacija: „…ovaj razgovor može biti sniman“. Specijalna bolnica je navela kako je razlog za korištenje navedene jezične formulacije „može biti sniman“ umjesto formulacije „ovaj razgovor se snima“ uslijed moguće kratkoće trajanja razgovora, a što je neosnovano. Naime, svi voditelji obrade osobnih podataka (ovdje Specijalna bolnica) kod bilo kakve obrade osobnih podataka dužni su proaktivno iskomunicirati prema ispitanicima jasnim, nedvosmislenim i razumljivim jezikom sva njihova prava iz Opće uredbe o zaštiti podataka, a što jasno traži članak 12. stavak 1. Opće uredbe o zaštiti podataka. Naime, intencija navedene odredbe je da se izbjegnu nejasne rečenične formulacije (npr. može) koje mogu ispitanicima ostaviti prostora za razna tumačenja te im tako ostaviti otvorena pitanja u pogledu obrade osobnih podataka. Upotrebom konstrukcije „može biti sniman“ ispitanici nisu bili sigurni u pogledu toga da li se razgovor snima ili se isti samo može snimati u pojedinim situacijama pa nisu niti znali na nedvosmislen način da li se obrađuju njihovi osobni podaci na takav način ili ne. Specijalna bolnica je trebala koristiti jasnu jezičnu formulaciju „ovaj razgovor se snima u svrhu…“ te bi takvim načinom bila poštivana odredba članka 12. stavka 1. Opće uredbe o zaštiti podataka, dok je na ovaj način došlo do kršenja iste. Naime, predmetni voditelj obrade osobnih podataka je ispitanicima sukladno obvezi informiranja još prije započete obrade osobnih podataka u vidu snimanja telefonskih razgovora trebao iskazati jasnu i izvedivu činjenicu snimanja razgovora u pogledu konkretne informacije o snimanju prije istoga.

Isto tako je utvrđeno kako Specijalna bolnica ima politiku privatnosti koja je dostupna i putem URL poveznice: https://www.medico.hr/o-nama/pravila-zastite-osobnih-podataka/. Pregledom navedene politike privatnosti, a koja je također dostavljena i Agenciji dopisom koji je zaprimljen u Agenciji dana 19. ožujka 2024. godine utvrđeno je kako se ista u niti jednom dijelu ne referira na obradu osobnih podataka odnosnu na snimanje telefonskih razgovora, a što je protivno odredbi članka 13. stavka 1. i 2. Opće uredbe o zaštiti podataka. Naime, svi voditelji obrade osobnih podataka su temeljem navedene odredbe u pravnoj obvezi proaktivno i transparentno informirati ispitanike, između ostalog, o svrsi pojedine obrade osobnih podataka i pravnoj osnovi, razdoblju pohrane takvih osobnih podataka, postojanju prava ispitanika u pogledu obrade osobnih podataka (npr. pristup podacima, ispravljanje podataka, pravo na prigovor, brisanje podataka). U konkretnom slučaju Specijalna bolnica kao voditelj obrade osobnih podataka nije naznačila da se snimaju telefonski razgovori upućeni prema pozivnom centru na broj 072 100 100, kao niti da se isti snimaju u svrhu unapređenja usluga niti temeljem koje pravne osnove. Ista također nije informirala ispitanike putem politike privatnosti niti o rokovima čuvanja osobnih podataka obrađenih putem snimanja telefonskih razgovora, zatim o postojanju prava ispitanika u pogledu njihovih snimki telefonskih razgovora. Iz netom

istaknutog jasno je utvrđeno kako Specijalna bolnica nije transparentno i proaktivno putem politike privatnosti informirala ispitanike o gore iznesenima aktivnostima obrade osobnih podataka odnosnim na snimanje telefonskih razgovora, odnosno kako im nije pružila informacije sukladno odredbi članka 13. stavka 1. točke (c) i stavka 2. točke (a) i (b) Opće uredbe o zaštiti podataka. Opisanim načinom detaljnije informacije o obradi osobnih podataka odnosnoj na snimanje telefonskih razgovora (izvan nejasnog upozorenja na početku telefonskog razgovora) su *de facto i de iure* održane u tajnosti te ispitanici nisu niti znali za elemente iz netom navedenih pravnih odredbi te su ostali uskraćeni za bitne informacije u pogledu moguće zaštite njihovih osobnih podataka. Dakle, Specijalna bolnica nije na transparentan način informirala ispitanike kako se njihovi podaci prikupljaju, čuvaju te na drugi način obrađuju.

U ovoj upravnoj stvari nadalje je utvrđeno kako je Specijalna bolnica u lipnju 2018. godine započela sa pregovorima u pogledu uspostave poslovne suradnje vezane uz implementaciju novog radiološkog informacijskog sustava te sustava za arhiviranje slika radioloških nalaza (RIS/PACS) kao i održavanje sustava te je Ugovor o poslovnoj suradnji (dalje u tekstu: ugovor) potpisan 28. studenog 2018. godine, a sustav je implementiran u Specijalnu bolnicu 01. ožujka 2019. godine. Iz ugovora (preslika istog prileži spisu predmeta) jasno proizlazi kako je predmet ugovora, između ostalog, migracija podataka iz starog sustava u novi kao i redovno održavanje radiološkog sustava RIS/PACS (što uključuje obradu osobnih podataka pacijenata u okviru sustava RIS/PACS) , a unutar kojeg ugovornog odnosa društvo Veridian kao što je to potvrđeno u nadzorima kod društva Veridian i kod Specijalne bolnice ima status izvršitelja obrade dok je Specijalna bolnica voditelj obrade osobnih podataka. U tom smislu u nadzoru kod društva Veridian i kod Specijalne bolnice je jasno utvrđeno kako zaseban ugovor ili aneks ugovora odnosan na obradu osobnih podataka u pogledu navedene usluge nije sklopljen, a što je bila pravna obveza voditelja obrade sukladno odredbi članka 28. stavka 3. Opće uredbe o zaštiti podataka da sklopi takav ugovor sa svim elementima iz navedenog članka, a što nije učinjeno te je navedenim propustom Specijalne bolnice došlo do povrede odredbi članka 28. stavka 3. Opće uredbe o zaštiti podataka.

Agencija je isto tako utvrdila kako Specijalna bolnica iz sustava radi dnevni backup (sigurnosne kopije) RIS i PACS baza podataka te da se iste nakon toga eksportiraju na decidiranu lokaciju unutar bolničke mreže, dok se back up (sigurnosne kopije) slikovne arhive iz radiološkog informacijskog sustava ne radi zbog velike količine podataka, a što bi iziskivalo veće resurse i ulaganja u informacijski sustav bolnice. U tom pogledu bitno je navesti kako je izrada sigurnosnih kopija neizostavni dio sigurnosnih mjera zaštite osobnih podataka i to tehničke prirode, a koje se moraju izrađivati osobito kod obrade posebnih kategorija osobnih podataka koje uživaju i posebnu zaštitu (što radiološki podaci o slikovnim datotekama pojedinih medicinskih radnji zasigurno predstavljaju). Izrada sigurnosnih kopija omogućuje kontinuiranu dostupnost osobnih podataka u slučaju njihovog gubitka, izmjene ili oštećenja te u tom smislu predstavlja neizostavnu mjeru očuvanja integriteta osobnih podataka te vrlo efikasan preventivni alat koji osigurava odgovarajuću razinu sigurnosti osobnih podataka. U ovom upravnom postupku utvrđeno je kako je Specijalna bolnica u srpnju 2019. godine izgubila neodređeni broj osobnih podataka u pogledu slikovnih datoteka u radiološkom informacijskom

sustavu, a upravo za čiji dio nisu izrađivane sigurnosne kopije. Da je postojala politika izrade sigurnosnih kopija tada bi ovakva vrsta gubitka osobnih podataka pacijenata Specijalne bolnice ne samo bila značajno smanjena već bi ista bila u potpunosti onemogućena te bi se osigurala cjelovitost i integritet osobnih podataka. Argumenti Specijalne bolnice kako sigurnosne kopije u dijelu slikovnih datoteka iz radiološkog informacijskog sustava nisu izrađivane iz razloga što bi to iziskivalo dodatne resurse te bi se radilo o velikim podatkovnim prostorima koje bi trebalo osigurati nisu prihvaćeni. Naime, svi voditelji obrade su sukladno odredbi članka 32. stavka 1. Opće uredbe o zaštiti podataka u obvezi provesti odgovarajuće mjere zaštite u odnosu na rizike na prava i slobode ispitanika kako bi se osigurala odgovarajuća razina sigurnosti osobnih podataka. Kada se radi o obradi posebnih kategorija podataka (ovdje osnovni identifikacijski podaci te posebna kategorija u pogledu zdravstvenih podataka) te mogućnosti njihova potpunog gubitka voditelji obrade su u obvezi da osiguraju dostupnost tih osobnih podataka sve dok traju rokovi njihova čuvanja sukladno posebnim propisima budući da potpuni i nepovratni gubitak osobnih podataka zdravstvene prirode može imati i snažnije reperkusije na opće zdravstveno stanje ispitanika čiji podaci su nepovratno izgubljeni budući da je kod zdravstvenih podataka iznimno bitna njihova cjelovitost, budući da gubitak samo jednog dijela zdravstvenih podataka može značiti da ispitanik ostaje bez rezultata pojedine pretrage, a koja ne može biti zamjenjiva. Naime, zdravstveni podaci odnosno nalazi koji su napravljeni u točno određenom trenutku s medicinske strane mogu biti iznimno bitni te nezamjenjivi kako bi se pojedini ispitanik mogao na adekvatni način liječiti te kako bi se moglo redovito pratiti stanje njegovog zdravstvenog stanja. Budući da su rizici netom izneseni itekako postojali Specijalna bolnica se ne može pozivati na troškove uspostave sigurnosnih kopija, budući da je ista kao voditelj obrade osobnih podataka koja obrađuje veći broj osobnih podataka od većeg broja ispitanika i to zdravstvene prirode dužna osigurati njihovu sigurnost te se postojanje sigurnosnih kopija ne može smatrati nesrazmjernim troškom u pogledu rizika od gubitka takvih podataka te je sigurnosna kopija u tom pogledu jedna od gotovo pa bazičnih mjera zaštite koja nije smjela biti ispostavljena u ovom slučaju. Budući da Specijalna bolnica nije uspostavila predmetne sigurnosne kopije dijela osobnih podataka svojih ispitanika ista je postupila protivno odredbi članka 32. stavka 1. Opće uredbe o zaštiti podataka.

U ovoj upravnoj stvari utvrđeno je i kako je Specijalna bolnica dana 23. srpnja 2019. godine nepovratno izgubila neodređeni broj osobnih podataka svojih ispitanika i to zdravstvene prirode (medicinske slike radioloških pretraga uz osnovne identifikacijske podatke) te kako je u tijeku nadzora od 29. veljače 2024. godine te kasnijim očitovanjima zauzela jasan stav kako su za gubitak podataka saznali tek nakon što su se ispitanici obratili Specijalnoj bolnici te zatražili pristup svojim osobnim podacima u obliku kopija. Nadalje, Agencija je u tijeku upravnog postupka izvršila uvid u popis prijavljenih sigurnosnih incidenata sukladno odredbama članka 33. stavka 1. Opće uredbe o zaštiti podataka te nije pronašla da je Specijalna bolnica prijavila navedeni incident. Specijalna bolnica se u tijeku upravnog postupka nije očitovala u pogledu prijave incidenta Agenciji. Iz netom iznesenog jasno je utvrđeno kako Specijalna bolnica nije prijavila sigurnosni incident gubitka osobnih podataka svojih pacijenata Agenciji u roku od 72 sata. Iz dodatnog očitovanja društva Veridian odnosno elektroničke korespondencije između X te glavne inženjerke radiologije Specijalne bolnice, a koja je upućena na adresu direktora Specijalne bolnice jasno proizlazi kako je Specijalna bolnica još 23. srpnja 2019. godine od

jutarnjih sati, a najkasnije od 23. srpnja 2019. godine u 12:25 sati saznala za sigurnosni incident nemogućnosti pristupa radiološkim podacima pacijenata u smislu da im je server na kojemu se nalaze osobni podaci nedostupan te da se ne može doći do osobnih podataka. Naime, u predmetnom sigurnosnom incidentu došlo je do nepovratnog gubitka osobnih podataka dijela ispitanika/pacijenata Specijalne bolnice i to u pogledu osnovnih identifikacijskih podataka kao i slikovnih nalaza UZV pregleda najmanje abdomena i dojki unutar radiološkog informacijskog sustava Specijalne bolnice. Nastavno na procjenu riziku potrebno je navesti kako se radilo o vrsti nepovratnog gubitka osobnih podataka (kako to navodi i Specijalna bolnica) iz radiološkog informacijskog sustava. Nadalje, radilo se o gubitku zdravstvenih podataka i to slika ultrazvučnih pretraga abdomena i dojki kao osobnih podataka posebne kategorije, a gubitak kojih već sam po sebi može značiti negativan utjecaj na prava i slobode ispitanika kao što je to već prethodno obrazloženo na stranici 14. ovog Rješenja. Kod procjene rizika također je potrebno kao mjerodavno uzeti u obzir i poseban položaj voditelja obrade koji obrađuje zdravstvene podatke kao podatke posebne kategorije, a koji su k tome još i iznimno osjetljive prirode te kod istog zasigurno postoji veća prijetnja za pojedince ako dođe do gubitka njihovih osobnih podataka. U odnosu na broj ispitanika zahvaćenih povredom u postupku je utvrđeno kako su izgubljeni podaci od najmanje 3 ispitanika (X, X, X – koji su se obratili Agenciji sa zahtjevom za utvrđivanje povrede prava) te kako se radilo o njihovom nepovratnom gubitku odnosno povredi njihove dostupnosti u najtežem obliku. Sve navedeno jasno ukazuje na postojanje visokog rizika po prava i slobode pacijenata te je Specijalna bolnica bila u obvezi prijaviti sigurnosni incident temeljem članka 33. stavka 1. Opće uredbe o zaštiti podataka, a što nije učinila te je na taj način povrijedila netom istaknutu odredbu odnosno pravnu obvezu.

Nadalje, također je utvrđeno kako službenica za zaštitu podataka nije bila uključena u izradu odnosno doradu politike privatnosti Specijalne bolnice, a koja je dostupna putem URL poveznice https://www.medico.hr/o-nama/pravila-zastite-osobnih-podataka/, kao niti u pitanja u pogledu obrade osobnih podataka putem snimanja razgovora s pozivnim centrom niti propisivanja rokova čuvanja takvih snimki te kako je njezin zadatak kao službenice za zaštitu podataka zaprimanje zahtjeva ispitanika za ostvarivanje njihovih prava te kako ostale poslove u pogledu pitanja primjene Opće uredbe o zaštiti podataka za Specijalnu bolnicu obavlja odvjetničko društvo Vukić i partneri iz Zagreba. Iz navedenog utvrđenja koje proizlazi iz Zapisnika o nadzoru od 07. ožujka 2024. godine jasno je kako službenica za zaštitu podataka nije na primjeren način bila uključena u sva pitanja u pogledu zaštite osobnih podataka i to kako u pogledu snimanja telefonskih razgovora, izrade/dorade politike privatnosti tako i ostalih pitanja vezanih uz usklađivanje s Općom uredbom o zaštiti podataka. Naime, jasno je kako odvjetničko društvo Vukić i partneri obavlja većinu poslova usklađivanja s Općom uredbom o zaštiti podataka (osim postupanja kod zahtjeva ispitanika kojima isti traže pristup osobnim podacima) te kako u takvim poslovima nije bila na primjeren način uključena službenica za zaštitu podataka. Opisanim načinom odnosno utvrđenjem propuštena je prilika da se osigura usklađivanje s Općom uredbom o zaštiti podataka na način da službenica za zaštitu podataka Specijalne bolnice bude aktivni sudionik u raspravi vezano uz sva pitanja (ne samo djelomična) koja uključuju obradu osobnih podataka. Specijalna bolnica nije dakle na adekvatan način uključila službenicu za zaštitu podataka u proces zaštite osobnih podataka i usklađivanje s Općom uredbom o zaštiti podataka odnosno ista nije uzela u obzir kako je upravo službenik za

zaštitu podataka osoba od koje se očekuje da vodi računa o cjelokupnoj primjeni Opće uredbe o zaštiti podataka Iz gore istaknutih razloga došlo je do povrede odredbi članka 38. stavka 1. Opće uredbe o zaštiti podataka.

II. UTVRĐENJE UPRAVNE NOVČANE KAZNE

Člankom 44. Zakona o provedbi Opće uredbe o zaštiti podataka (dalje u tekstu: Zakon) je propisano da Agencija izriče upravne novčane kazne za povrede odredaba ovoga Zakona i Opće uredbe o zaštiti podataka, sukladno članku 83. Opće uredbe o zaštiti podataka.

Člankom 45. stavkom 1. navedenog Zakona je propisano da se upravne novčane kazne izriču odlukom. Temeljem stavka 2. istoga članka, odlukom će se utvrditi iznos i način uplate upravne novčane kazne. Odlukom se može utvrditi da se upravna novčana kazna plaća u obrocima. Temeljem stavka 4. istoga članka, protiv odluke nije dopuštena žalba, ali se može pokrenuti upravni spor pred nadležnim upravnim sudom.

Temeljem članka 46. istoga Zakona, upravna novčana kazna uplaćuje se u roku od 15 dana od dana pravomoćnosti odluke kojom je izrečena. Ako stranka u propisanom roku ne uplati upravnu novčanu kaznu odnosno po dospijeću zadnjeg obroka ako je odobreno obročno plaćanje, Agencija će obavijestiti Područni ured Porezne uprave Ministarstva financija na čijem je području prebivalište odnosno sjedište stranke kojoj je izrečena upravna novčana kazna, radi naplate upravne novčane kazne prisilnim putem prema propisima o prisilnoj naplati poreza. Upravne novčane kazne uplaćuju se u korist državnog proračuna. Iznimno od stavka 2. ovoga članka, na dospjelu, a neplaćenu upravnu novčanu kaznu ne obračunava se kamata.

S obzirom na utvrđene okolnosti u konkretnom slučaju Agencija je sukladno svojim ovlastima iz članka 58. stavka 2. točke (i) Opće uredbe o zaštiti podataka izrekla upravnu novčanu kaznu umjesto drugih korektivnih mjera iz predmetnog članka, a sve u skladu s uvjetima za njezino izricanje iz članka 83. Opće uredbe o zaštiti podataka i članka 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka. Nakon detaljnog razmatranja raspoloživih korektivnih mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka, a koje nadzorno tijelo ima ovlasti izreći voditelju obrade, u slučaju kršenja odredbi Opće uredbe o zaštiti podataka, te cijeneći sve okolnosti predmetnog slučaja, a posebno da odabrana korektivna mjera mora biti učinkovita, proporcionalna i odvraćajuća u svakom pojedinom slučaju, Agencija je odlučila izreći upravnu novčanu kaznu posvećujući dužnu pozornost kriterijima propisanim člankom 83. stavkom 2. Opće uredbe o zaštiti podataka.

Naime, člankom 83. stavkom 1. Opće uredbe o zaštiti podataka propisano je da svako nadzorno tijelo osigurava da je izricanje upravnih novčanih kazni u skladu s ovim člankom u pogledu kršenja ove Uredbe iz stavaka 4., 5. i 6. u svakom pojedinačnom slučaju učinkovito, proporcionalno i odvraćajuće.

Agencija smatra da iznos izrečene upravne novčane kazne ne može biti učinkovit ako nema značajan utjecaj na prihode voditelja obrade, načelo proporcionalnosti ne može se održati ako se povreda razmatra apstraktno bez obzira na utjecaj na voditelja ili izvršitelja obrade, a ista treba biti i odvraćajuća od budućih kršenja. Dakle, izrečena upravna novčana kazna ne može biti odvraćajuća ako nema financijskog utjecaja na predmetnog voditelja obrade.

Izricanjem upravne novčane kazne ujedno se želi postići da se poštuju pravila o zaštiti osobnih podataka kako od strane samog voditelja obrade tako i od svih drugih voditelja/izvršitelja obrade koji obrađuju osobne podatke ispitanika. Izricanjem upravne novčane kazne treba se postići generalno odvraćanje (obeshrabriti druge u ponavljanju istog kršenja u budućnosti), kao i posebno odvraćanje (obeshrabriti adresata ove upravne novčane kazne od ponavljanja istog kršenja).

Temeljem članka 83. stavka 2. Opće uredbe o zaštiti podataka, upravne novčane kazne izriču se uz mjere ili umjesto mjera iz članka 58. stavka 2. točaka od (a) do (h) i članka 58. stavka 2. točke (j), ovisno o okolnostima svakog pojedinog slučaja. Pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne u svakom pojedinom slučaju dužna se pozornost posvećuje sljedećem:

(a) prirodi, težini i trajanju kršenja, uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli;
(b) ima li kršenje obilježje namjere ili nepažnje;
(c) svakoj radnji koju je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici;
(d) stupnju odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32.;
(e) svim relevantnim prijašnjim kršenjima voditelja obrade ili izvršitelja obrade;
(f) stupnju suradnje s nadzornim tijelom kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja;
(g) kategorijama osobnih podataka na koje kršenje utječe;
(h) načinu na koji je nadzorno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri voditelj obrade ili izvršitelj obrade izvijestio o kršenju;
(i) ako su protiv dotičnog voditelja obrade ili izvršitelja obrade u vezi s istim predmetom prethodno izrečene mjere iz članka 58. stavka 2., poštovanju tih mjera;
(j) poštovanju odobrenih kodeksa ponašanja u skladu s člankom 40. ili odobrenih mehanizama certificiranja u skladu s člankom 42.; i
(k) svim ostalim otegotnim ili olakotnim čimbenicima koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem.

U članku 83. stavku 5. točki (b) Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade u pogledu ostvarivanja prava ispitanika iz članaka 12. do 22. Opće uredbe o zaštiti podataka mogu izreći upravne novčane kazne u iznosu do 20 000 000

EUR, ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.

Uvodnom izjavom 150 Opće uredbe o zaštiti podataka definira se da u slučaju kada se upravne novčane kazne izriču poduzetniku, poduzetnik bi se u te svrhe trebao tumačiti u skladu s člankom 101. i 102. Ugovora o funkcioniranju Europske unije.

Uvidom u podatke iz sudskog registra Agencija je utvrdila da je osnivač Specijalne bolnice društvo ERGOMED, društvo s ograničenom odgovornošću za zastupanje, proizvodnju i usluge, pod MBS: 080184576, upisan kod: Trgovački sud u Zagrebu, OIB: 19373775802, Zagreb, Gračanska 12. Nadalje, isto tako je utvrđeno iz godišnjeg financijskog izvještaja kojeg je FINA dostavila Agenciji kako je Specijalna bolnica u 2023. godini ostvarila 9,11 milijuna Eura ukupnih prihoda. Budući da ukupni godišnji promet (na dan pisanja Rješenja) iznosi 9.110.000,00 Eura, 4 % tog iznosa je 364.400,00 Eura, 4, dok je 190.000,00 Eura 2.09 % od ukupnog godišnjeg prometa.

364.400,00 Eura predstavlja 4 % od gore navedenog ukupnog prometa, te budući da isti iznosi manje od 20.000.000,00 Eura, gornju granicu za izricanje upravne novčane kazne u konkretnom slučaju predstavlja iznos od 20.000.000,00 Eura, a uzimajući u obzir utvrđene povrede.

Na temelju odredbe članka 83. stavka 2. Opće uredbe o zaštiti podataka, pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne, Agencija je u ovom slučaju dužnu pozornost posvetila sljedećem:

- Priroda, težina i trajanje kršenja, uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli (članak 83. stavak 2, točka a);

U predmetnom slučaju, kako je utvrđeno u točki I. izreke ovog rješenja, Specijalna bolnica nije na odgovarajući način propisala rokove čuvanja osobnih podataka koji su prikupljeni putem snimki razgovora s pozivnim centrom dostupnim putem broja 072 100 100 te je time došlo do zadržavanja osobnih podataka protivno članku 5. stavku 1. točki (e) Opće uredbe o zaštiti podataka i to u odnosu na barem 435 909 ispitanika čiji podaci su dostupni Specijalnoj bolnici u aplikativnom dijelu. U tom pogledu isto tako je utvrđeno kako je povreda trajala od 25. svibnja 2018. godine te kako traje i dalje budući da Specijalna bolnica još uvijek nije propisala rokove čuvanja osobnih podataka iz predmetne obrade. Opisana povreda se odnosila isključivo na područje Republike Hrvatske te u postupku nije utvrđeno da su ispitanici na taj način pretrpjeli štetu. Isto tako je utvrđeno kako se u pogledu svrhe obrada odnosila na redovito kontaktiranje ispitanika u svrhu dogovaranja termina za medicinske preglede, odnosno da je obrada bila gotovo u samoj srži vezanoj uz osnovnu djelatnost Specijalne bolnice, a što dodatno daje na težini povrede, budući da bi tako veliki voditelj obrade čija je osnovna djelatnost vezana uz pružanje medicinskih usluga trebalo posvetiti posebnu pozornost pitanjima obrade osobnih podataka koja je vezana uz jednu od temeljnih djelatnosti voditelja obrade.

Nadalje, točkom II. izreke ovog Rješenja utvrđeno je kako Specijalna bolnica nije dokazala postojanje pravne osnove za obradu osobnih podataka prikupljenih putem snimki telefonskih razgovora s pozivnim centrom te za ostale elemente iz članka 83. stavka 2. točke (a) Opće uredbe o zaštiti podataka vrijedi sve što je napisano za točku iznad u pogledu propisivanja rokova čuvanja snimki, tako i u pogledu točke III. izreke Rješenja odnosno transparentnosti te korištenja jasnog i nedvosmislenog jezika kod takve obrade osobnih podataka.

U pogledu (ne)sklapanja ugovora o obradi osobnih podataka s društvom Veridian kao izvršiteljem obrade osobnih podataka iz točke IV. izreke Rješenja u postupku je utvrđeno kako se radilo o implementaciji novog radiološkog informacijskog sustava te sustava za arhiviranje slika radioloških nalaza (RIS/PACS) kao i održavanje sustava te kako je opisanim načinom neizravno došlo do ugrožavanja sigurnosti osobnih podataka ispitanika Specijalne bolnice čiji osobni podaci su sadržani u RIS/PACS radiološkom sustavu (o čijem točnom broju se Specijalna bolnica na višekratne upite nije izjasnila te je navedeno uzeto u obzir kao neutralna okolnost), budući da je sklapanje ugovora s izvršiteljem obrade jedna od svojevrsnih sigurnosnih poluga koja osigurava da se znaju pravila obrade osobnih podataka te njihov tijek u poslovnom odnosu između voditelja i izvršitelja obrade te kako bi se voditelj obrade uistinu osigurao da izvršitelj obrade zadovoljava tehničke i organizacijske mjere zaštite kod obrade osobnih podataka velikog broja ispitanika, budući da angažiranje izvršitelja obrade može predstavljati svojevrsni sigurnosni izazov pri obradi osobnih podataka, jer se na taj način u lanac obrade osobnih podataka dodaje još jedna karika te samim time rastu izazovi osiguranja odgovarajućih tehničkih i organizacijskih mjera zaštite osobnih podataka ispitanika. Utvrđeno je kako je navedena povreda trajala najmanje od implementacije sustava odnosno od 01. ožujka 2019. godine 2019. godine te traje i dalje budući da je navedeni poslovni odnos i dalje aktivan. Obrada osobnih podataka unutar navedenog poslovnog odnosa je ograničena na područje Republike Hrvatske te nije utvrđeno postojanje štete po ispitanike zbog nepostojanja ugovora o obradi osobnih podataka. Nastavno na svrhu u postupku je utvrđeno kako se radilo o pružanju usluga vezanih uz rad radiološkog informacijskog sustava na kojemu se nalaze zabilježeni osobni podaci ispitanika/pacijenata odnosno utvrđeno je kako se radi o jednoj od temeljnih djelatnosti Specijalne bolnice koja je izravno vezana uz čuvanje osobnih podataka koji su nastali u procesu pružanja medicinskih/radioloških usluga.

Nastavno na točku V. izreke Rješenja odnosno nepoduzimanje odgovarajućih tehničkih mjera zaštite utvrđeno je kako je predmetna obrada također bila vezana isključivo uz područje Republike Hrvatske te kako se radilo o jednoj od temeljnih djelatnosti Specijalne bolnice odnosno o čuvanju zdravstvenih osobnih podataka na radiološkom informacijskom sustavu u pogledu slikovnih radioloških datoteka za koje se nisu izrađivale sigurnosne kopije i to od 25. svibnja 2018. godine odnosno stupanja na snagu i obvezujuće primjene Opće uredbe o zaštiti podataka. U odnosu na broj ispitanika zbog ne dostavljanja takvih podataka isto je uzeto kao neutralna okolnost. Također je utvrđeno kako ispitanici nisu pretrpjeli izravnu materijalnu ili nematerijalnu štetu uslijed nepoduzimanja odgovarajućih mjera zaštite no kako takva šteta posljedično može nastati budući da su medicinski podaci u pogledu njihove cjelovitosti iznimno bitni za zaštitu zdravlja ispitanika, a što je objašnjeno na stranici 15. ovog Rješenja.

Točkom VI. izreke Rješenja utvrđeno je kako Specijalna bolnica nije prijavila sigurnosni incident gubitka osobnih podataka Agenciji kao nadzornom tijelu te je u postupku utvrđeno kako je predmetnim incidentom uključeno najmanje 3 ispitanika te kako je do gubitka podataka došlo 23. srpnja 2019. godine, a o čemu je navedenog dana saznanja imala i inženjerka radiologije kao i uprava Specijalne bolnice koja je o tome obaviještena od strane društva Veridian. Navedeni incident se odnosio isključivo na područje Republike Hrvatske te uslijed istog nije utvrđena materijalna ili nematerijalna šteta po ispitanike. Kao i za prethodnu točku radilo se o jednoj od temeljnih djelatnosti Specijalne bolnice.

U pogledu točke VII. izreke Rješenja utvrđeno je kako službenica za zaštitu podataka Specijalne bolnice nije bila na odgovarajući način uključena u sva pitanja u pogledu zaštite osobnih podataka te je navedena povreda bila ograničena na područje Republike Hrvatske. U pogledu svrhe utvrđeno je kako se nije radilo isključivo o temeljnoj djelatnosti Specijalne bolnice, ali kako su pitanja vezana uz obradu osobnih podataka u svojoj ukupnosti u pojedinim dijelovima ipak vezana uz temeljnu djelatnost obrade zdravstvenih podataka te je službenica za zaštitu podataka zasigurno mogla na odgovarajući način dati svoj aktivni doprinos zaštiti osobnih podataka svih ispitanika Specijalne bolnice da je bila uključena u sva, a ne samo parcijalna pitanja obrade osobnih podataka Specijalne bolnice. Predmetna povreda traje od 2019. godine od kada je predmetna službenica za zaštitu podataka imenovana, a budući da nije utvrđen točan datum imenovanja za službenicu za zaštitu podataka, kao dan će se uzeti 31. prosinca 2019. godine te povreda traje i dalje.

- Ima li kršenje obilježje namjere ili nepažnje (članak 83. stavak 2, točka b);

Nastavno na propisivanje rokova čuvanja osobnih podataka koji su obrađeni putem snimki telefonskih razgovora iz točke I. izreke ovog Rješenja, a u pogledu oblika krivnje u postupku je utvrđeno kako se radilo o nepoznavanju Opće uredbe o zaštiti podataka u dijelu kojim se traži jasno propisivanje rokova čuvanja u minimalno potrebnom vremenskom periodu iz članka 5. stavka 1. točke (e) Opće uredbe o zaštiti podataka, a što je potvrđeno u kasnijem tijeku postupka kada je Specijalna bolnica u očitovanju koje je zaprimljeno u Agenciji 19. ožujka 2024. godine navela kako takve podatke namjeravaju čuvati sukladno odredbama Zakona o liječništvu pa je iz svega razvidno kako se radilo o nepažnji, a ne namjeri Specijalne bolnice u pogledu rokova čuvanja. Specijalna bolnica je trebala biti svjesna navedene pravne obveze.

Nastavno na točku II. izreke Rješenja odnosno pravnu osnovu za snimanje telefonskih razgovora odnosno osobnih podataka sadržanih u njima u postupku je utvrđeno kako se također radilo nepoznavanju Opće uredbe o zaštiti podataka, a što je posebno utvrđeno iz izjave službenice za zaštitu podataka dane u nadzoru od 29. veljače 2024. godine kada je na posebno postavljeno pitanje ovlaštenog službenika Agencije da dokaže postojanje pravne osnove za snimanje telefonskih razgovora s ispitanicima ista upitala ovlaštenog službenika Agencije da joj navede koje sve pravne osnove postoje u Općoj uredbi o zaštiti podataka. Nadalje, Specijalna bolnica je trebala biti svjesna svoje pravne obveze da dokaže pravnu osnovu za takvu vrstu obrade osobnih podataka, a osobito uzimajući u obzir činjenicu da imaju imenovanu službenicu

za zaštitu podataka. Dakle, i iz netom navedene točke izreke Rješenja jasno proizlazi neznanje Specijalne bolnice u pogledu dokazivanja pravne osnove za snimanje telefonskih razgovora.

U pogledu točke III. izreke Rješenja utvrđeno je kako Specijalna bolnica nije informirala ispitanike o obradi njihovih osobnih podataka na odgovarajući način detaljno obrazložen gore u Rješenju te kako je ista trebala biti svjesna (uzimajući u obzir njezine kapacitete i vrstu osobnih podataka koje obrađuje) o svojoj obvezi informiranja ispitanika, ali kako se radi o neznanju odnosno nepoznavanju Opće uredbe o zaštiti podataka odnosno kako je riječ o nepažnji Specijalne bolnice.

Nastavno na točku IV. izreke Rješenja utvrđeno je kako se također radilo o neznanju Specijalne bolnice kao voditelja obrade da je dužna sklopiti ugovor o obradi osobnih podataka s društvom Veridian kao izvršiteljem obrade za gore navedenu uslugu te kako je ista trebala biti svjesna da je dužna sklopiti takav ugovor uzimajući u obzir gore iznesena utvrđenja u pogledu utvrđenja nepažnje.

U odnosu na točku V. izreke Rješenja u postupku je utvrđeno kako Specijalna bolnica nije poduzela odgovarajuće tehničke mjere zaštite u pogledu radiološkog informacijskog sustava i to u dijelu slikovnih datoteka za koje nisu izrađivane sigurnosne kopije. Također je kao relevantno utvrđeno kako se radilo o namjernom postupanju budući da je Specijalna bolnica znala kako se ne rade sigurnosne kopije te je svjesno zanemarila takvu svoju obvezu pozivajući se na utrošak resursa u uspostavi takve sigurnosne mjere zaštite osobnih podataka. Naime, pozivanje na nedostatak resursa nikako ne može biti opravdanje budući da bi voditelji obrade trebali biti odgovorni za određivanje svih resursa koji su potrebni za zaštitu osobnih podataka uzimajući u obzir rizike od obrade te ovisno o prirodi i složenosti njihova poslovanja, a koja priroda je iznimno složena kod Specijalne bolnice te iziskuje potrebu za snažnijim mjerama zaštite dok je uspostava sigurnosnih kopija mjera koja u niti jednom pogledu nije nerazumna uzimajući u obzir cjelokupni kontekst obrade osobnih podataka.

Nastavno na točku VI. izreke Rješenja u postupku je utvrđeno kako Specijalna bolnica nije imala znanja da je u obvezi prijaviti sigurnosni incident po članku 33. stavku 1. Opće uredbe o zaštiti podataka iako je navedenu svijest trebala imati i biti svjesna svoje obveze po Općoj uredbi o zaštiti podataka te je navedeno uzeto u obzir kao nepažnja po načelu *in dubio pro reo* zbog nedostatka dokaza o namjeri.

Kod točke VII. izreke Rješenja također je zbog neznanja i nedostatka svijesti koja je trebala biti razvijena kod Specijalne bolnice došlo do neuključivanja službenice za zaštitu podataka u sva pitanja obrade osobnih podataka te se radilo o nepažnji.

- Svaka radnja koju je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici (članak 83. stavak 2., točka c);

Nastavno na sve točke u pogledu snimanja telefonskih razgovora od točke I. do točke III. izreke Rješenja Specijalna bolnica nije obavijestila Agenciju da je poduzimala bilo kakve radnje u

pogledu ispravljanja uočenih nepravilnosti kod takve vrste obrade osobnih podataka te je i predmetna politika privatnosti i dalje u identičnom sadržaju kao i prije nadzora od 29. veljače 2024. godine. Agencija također nije zaprimila nikakve informacije od Specijalne bolnice da je promijenila uvodnu poruku u pogledu mogućnosti snimanja telefonskih razgovora preko pozivnog centra.

U pogledu ne sklapanja ugovora o obradi osobnih podataka s izvršiteljem obrade društvom Veridian Agencija također nije zaprimila informacije da bi navedeni ugovor bio u međuvremenu sklopljen.

Nadalje, u pogledu poduzimanja odgovarajućih mjera zaštite Agencija također nije zaprimila informaciju da bi sustav sigurnosnih kopija bio uspostavljen na gore opisani način.

U odnosu na prijavu sigurnosnog incidenta utvrđeno je kako nije moguće naknadno poduzimanje takve radnje te se takva okolnost nije uzela u obzir prilikom izricanja visine kazne.

Nastavno na uključenost službenice za zaštitu podataka u sva pitanja vezana uz obradu osobnih podataka Agencija nije zaprimila informacije o njezinom povećanom angažmanu na pitanjima obrade osobnih podataka dok navedena okolnost nije utjecala na podizanje visine izrečene upravno novčane kazne.

- Stupanj odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32. (članak 83. stavak 2 točka d);

Specijalna bolnica snosi visoki stupanj odgovornosti uzimajući u obzir tehničke mjere zaštite budući da je izrada sigurnosnih kopija jedan od najboljih preventivnih alata koji ima za cilj osigurati kontinuiranu dostupnost i cjelovitost osobnih podataka, a što bolnica nije poduzela. No, kako se radi o okolnosti za koju je utvrđena povreda po točki V. izreke Rješenja, Agencija nije navedenu okolnost dodatno uzela u obzir kod visine izrečene upravno novčane kazne.

- Relevantna prijašnja kršenja voditelja obrade ili izvršitelja obrade (članak 83. stavak 2. točka e);

Prema evidencijama kršenja koje vodi ova Agencija, ista nije utvrdila prethodna kršenja Opće uredbe o zaštiti podataka od strane Specijalne bolnice u periodu od 25. svibnja 2018. godine te je navedeno uzeto u obzir kao olakotna okolnost kod izricanja visine kazne. No, Agencija je dana 17. srpnja 2017. godine donijela Rješenje (KLASA: UP/I-041-02/17-08/13), a kojim je utvrdila nezakonitost obrade osobnih podataka u pogledu obrade otiska prste i fotografije lica u svrhu evidencije vođenja radnog vremena od strane Specijalne bolnice. Agencija je u pogledu netom navedenog Rješenja uzela u obzir da se radilo o relativno kraćem vremenskom odmaku od predmetne povrede (povreda je bila utvrđena 2017. godine, dok su povrede u ovom Rješenju od 25. svibnja 2018. godine) te je navedeno uzeto u obzir kao otegotna okolnost kod izricanja visine upravno novčane kazne kao dokaz kontinuiteta kršenja propisa o zaštiti osobnih

podataka, No, isto tako predmetna otegotna okolnost nije u većoj mjeri utjecala na visinu kazne iz razloga što se radilo o povredi temeljem nacionalnog propisa donesenog na temelju Direktive 95/46, a koja više nije na snazi, već je u manjoj samo mjeri doprinijela predmetnoj visini upravno novčane kazne. Po prirodi povrede radilo se o istovrsnim kršenjima budući da se povreda odnosila na postojanje pravne osnove za obradu osobnih podataka, a kao što je to slično utvrđeno u točki II. izreke ovog Rješenja.

- Stupanj suradnje s nadzornim tijelom kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja (članak 83. stavak 2. točka f);

Specijalna bolnica je u tijeku nadzornih postupanja te čitavog upravnog postupka u većoj mjeri odgovarala na zahtjeve nadzornog tijela, odnosno Agencije, no isto tako su utvrđene određene manjkavosti kod suradnje, a što je uzeto u obzir kao otegotna okolnost. Naime, Specijalna bolnica nije u cijelosti govorila istinu kod datuma saznanja za sigurnosni incident te je tvrdila kako je za gubitak podataka saznala tek nakon što su se pojedini ispitanici obratili sa zahtjevima za ostvarivanje prava na pristup podacima odnosno u rujnu 2022. godine, dok je u postupku utvrđeno suprotno. Konkretnije, Agencija je u tijeku upravnog postupka došla u posjed preslike elektroničke korespondencije između predstavnika društva Veridian kao izvršitelja obrade i uprave Specijalne bolnice, a iz koje je razvidno kako je glavna inženjerka radiologije još 23. srpnja 2019. godine došla do saznanja kako se ne može pristupiti serveru radiološkog sustava na kojemu se nalaze slikovne datoteke pacijenata odnosno kako se ne može doći do inicijalizacije memorije (nedostupnost osobnih podataka) te je društvo Veridian o svemu obavijestilo upravu Specijalne bolnice te navedena elektronička korespondencija prileži spisu predmeta.

- Kategorije osobnih podataka na koje kršenje utječe (članak 83. stavak 2. točka g);

U ovoj upravnoj stvari utvrđena je obrada osnovnih identifikacijskih podataka kao i podataka o slikovnim datotekama na kojima su sadržani prikazani medicinskog stanja ispitanika kao posebne kategorije podataka te u pogledu snimki telefonskih razgovora i podaci o boji glasa (zdravstveni podaci).

- Način na koji je nadzorno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri voditelj obrade ili izvršitelj obrade izvijestio o kršenju (članak 83. stavak 2. točka h);

Agencija je od dana 21. studenog 2022. godine zaprimila više zahtjeva za utvrđivanje povrede prava na zaštitu osobnih podataka zbog ostvarivanja prava na pristup podacima, a u kojima je bilo navedeno kako su ispitanici od Specijalne bolnice nakon što su tražili pristup svojim zdravstvenim podacima obaviješteni kako su njihovi podaci nepovratno izgubljeni zbog kvara na serveru u srpnju 2019. godine te kako uslijed gubitka podataka ne mogu ostvariti njihovo prava na pristup osobnim podacima. Dakle, Specijalna bolnica nije proaktivno informirala Agenciju o gubitku podataka već je to Agencija saznala od strane ispitanika, ali s obzirom da je o tome utvrđena povreda u točki VI. izreke ovog Rješenja, navedena okolnost nije dodatno uzeta u obzir kao otegotna. U pogledu ostalih okolnosti od točke I. do V. te točke VII. Agencija

je navedene povrede saznala u tijeku obavljanja svojih nadzornih ovlasti po službenoj dužnosti te su se takve okolnosti vrednovale kao neutralne i nisu utjecale na visinu izrečene upravno novčane kazne.

- Ako su protiv dotičnog voditelja obrade ili izvršitelja obrade u vezi s istim predmetom prethodno izrečene mjere iz članka 58. stavka 2., poštovanju tih mjera (članak 83. stavak 2. točka i);

Specijalnoj bolnici Medico u vezi s istim predmetom prethodno nije izrečena nikakva mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka, a što je olakotna okolnost.

- Poštovanje odobrenih kodeksa ponašanja u skladu s člankom 40. ili odobrenih mehanizama certificiranja u skladu s člankom 42. (članak 83. stavak 2. točka j);

Nije primjenjivo u predmetnom slučaju.

- Svi ostali otegotni ili olakotni čimbenici koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem (članak 83. stavak 2. točka k);

Od ostalih otegotnih čimbenika zasigurno je uzeta u obzir činjenica kako je 23. srpnja 2019. godine došlo do nepovratnog gubitka osobnih podataka, a što je posljedica nepoduzimanja odgovarajućih tehničkih mjera zaštite. Naime, Agenciji je za utvrđenje povrede članka 32. Opće uredbe o zaštiti podataka bitno utvrditi i dokazati da voditelj obrade osobnih podataka nije implementirao odgovarajuće zaštitne mjere kao vrstu preventivnih alata koji imaju za cilj sprječavanje (u ovom slučaju) gubitka osobnih podataka odnosno koji mogu osigurati stalnu dostupnost osobnih podataka na sekundarnoj lokaciji neovisno o njihovom gubitku na primarnoj lokaciji. Činjenica gubitka osobnih podataka zasigurno predstavlja svojevrsni sigurnosni incident, ali se isti veže kao dodatna posljedica nepoduzimanja sigurnosnih mjera zaštite koje su razlog za utvrđenje povrede, dok gubitak predstavlja otegotnu okolnost budući da je zbog nepoduzimanja mjera zaštite u preventivnoj fazi kasnije došlo do reakcije u pogledu gubitka podataka, a što predstavlja otegotnu okolnost koju je Agencija uzela u obzir kod izračuna visine upravno novčane kazne.

Uzeta je u obzir (kao otegotna okolnost) činjenica kako se radi o jednoj od vodećih privatnih bolnica na području Republike Hrvatske koja je bila i začetnik privatne prakse u pružanju zdravstvenih usluga 1991. godine (podaci dostupni putem URL poveznice: https://www.medico.hr/o-nama/) te je ista danas jedan od regionalnih lidera u području pružanja zdravstvenih usluga, a koja pruža medicinske usluge iz gotovo svih grana medicine te svakodnevno obrađuje velike količine osobnih podataka i to zdravstvene prirode kao posebne kategorije podataka (koja je pri tome i materijalno i formalno kapacitirana da odgovori izazovima koje stavlja pred voditelje obrade Opća uredba o zaštiti podataka) te je samim time trebala biti svjesnija nužnosti bolje zaštite osobnih podataka svojih ispitanika kao i nužnosti njihovog odgovarajućeg informiranja, propisivanja rokova čuvanja podataka, dokazivanja

pravne osnove, prijave sigurnosnog incidenta, sklapanja ugovora o obradi osobnih podataka s izvršiteljem obrade i cjelovite uključenosti službenice za zaštitu podataka u sva pitanja obrade osobnih podataka.

Potrebno je ukazati kako će predmetnim iznosom kazne biti postignuta osim generalne i specijalna prevencija na način da će se odvratiti predmetni voditelj obrade osobnih podataka od sličnog kršenja Opće uredbe o zaštiti podataka u budućnosti te kako će svi izravni i neizravni adresati postati svjesni nužnosti poštivanja propisa o zaštiti osobnih podataka, a osobito u dijelu poštivanja obveze primjene odgovarajućih tehničkih i organizacijskih mjera zaštite, potrebe dokazivanja pravne osnove kod obrade osobnih podataka, propisivanja rokova čuvanja osobnih podataka, sklapanja ugovora s izvršiteljem obrade, transparentnog informiranja ispitanika, prijavljivanja sigurnosnih incidenata, kao i uključenosti službenika za zaštitu podataka u sva pitanja vezana uz obradu osobnih podataka. Isto tako, svaka kazna mora biti i efikasna u pogledu utjecaja na konkretnog voditelja obrade osobnih podataka, a kojemu se ne smije „isplatiti“ kršenje odredbi Opće uredbe o zaštiti podataka, već mu se mora kaznom koja je primjerena njegovim financijskim prilikama (gore objašnjeno), kao i povredi u pitanju (proporcionalnost) jasno dati do znanja da je neprihvatljivo višestruko kršenje Opće uredbe o zaštiti podataka koje je bilo predmetom ovog upravnog postupka. Agencija smatra kako se radi o financijski dobro stojećem voditelju obrade koji je u predmetnom slučaju učinio više povreda Opće uredbe o zaštiti podataka. Uzimajući u obzir sve gore navedene parametre te otegotne i olakotne okolnosti utvrđivanja pojedine upravne novčane kazne, kao i poštujući kazne koje su u sličnim činjeničnim stanjima izrekla druga nadzorna tijela u okviru mehanizma konzistentnosti te Agencije u svojoj praksi, ista smatra kako je utvrđeni iznos kazne od 190.000,00 Eura prikladan za postizanje svrhe kažnjavanja u ovom slučaju, odnosno da je kazna učinkovita, proporcionalna i odvraćajuća u ovoj upravnoj stvari, te da je njezin iznos u potpunosti primjeren okolnostima konkretnog slučaja.

Zaključno, Agencija nije odlučila izreći drugu blažu korektivnu mjeru (uključujući službenu opomenu) budući da je riječ o kršenju višestrukih odredbi Opće uredbe o zaštiti podataka i to od strane jedne od vodećih privatnih zdravstvenih ustanova na području Republike Hrvatske, a koja si nije smjela dopustiti ovakvo postupanje, a osobito u pogledu mjera zaštite da ne uspostavi sustav sigurnosnih kopija nad radiološkim informacijskim sustavom u kojem se pohranjuju slikovne datoteke ispitanika, odnosno njihovi osobni podaci te je navedeno nakon kvara na serveru koji se dogodio 23. srpnja 2019. godine dovelo do toga da se osobni podaci ispitanika u pogledu slikovnih datoteka više ne mogu obnoviti jer nije bilo alternativne/sekundarne lokacije pohrane takvih podataka, a koja bi se mogla iskoristiti u slučaju kvara na primarnom serveru, a što je ovdje bio slučaj. Kršenje Opće uredbe o zaštiti podataka se odnosilo i na same temelje Opće uredbe o zaštiti podataka, budući da u pogledu gore navedenih (izreka Rješenja) obrada osobnih podataka nije dokazano postojanje pravne osnove za snimanje telefonskih razgovora te ispitanici o pojedinim aktivnostima obrade osobnih podataka nisu bili na odgovarajući način informirani. Agencija je slijedom svega gore navedenog bila dužna izreći upravnu novčanu kaznu kao korektivnu mjeru u ovoj upravnoj stvari.

Slijedom navedenog odlučeno je kao u Izreci rješenja.

UPUTA O PRAVNOM LIJEKU

Protiv ovog rješenja žalba nije dopuštena, ali se može pokrenuti upravni spor pred Upravnim sudom u Rijeci u roku od 30 dana od dana dostave rješenja.

ZAMJENIK RAVNATELJA

Igor Vulje

1. Odvjetnički ured Vukić i partneri, Nikole Tesle 9, 51 000 Rijeka
2. Pismohrana, ovdje