



P/

**REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA**

KLASA:
URBROJ:
Zagreb,

Agencija za zaštitu osobnih podataka (OIB: 28454963989), na temelju članka 57. stavka 1., članka 58. stavka 1. i 2. točke (i) i članka 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) SL EU L119, članka 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka ("Narodne novine" br. 42/18) te članka 42. stavka 1. i 2. i članka 96. Zakona o općem upravnom postupku ("Narodne novine" br. 47/09, 110/21) u postupku pokrenutom po službenoj dužnosti, donosi sljedeće:

R J E Š E N J E

1. Utvrđuje se da ustanova Bolnica X iz __, kao voditelj obrade, u razdoblju od svibnja 2018. do rujna 2024. nije ispitanicima pružila informacije o obradi osobnih podataka, sukladno obvezi iz članka 13. Opće uredbe o zaštiti podataka.
2. Utvrđuje se da ustanova Bolnica X iz __ kao voditelj obrade, nije na odgovarajući način provodila i testirala organizacijske mjere zaštite koje imaju za cilj osiguranje sigurnosti obrade zdravstvenih podataka, sukladno obvezi iz članka 32. Opće uredbe o zaštiti podataka.
3. Utvrđuje se da ustanova Bolnica X iz __ kao voditelj obrade, nije izvijestila Agenciju za zaštitu osobnih podataka o povredi osobnih podataka u roku od 72 sata od saznanja za istu, sukladno obvezi iz članka 33. Opće uredbe o zaštiti podataka.
4. Utvrđuje se da ustanova Bolnica X iz __ kao voditelj obrade, nije izvijestila ispitanika čiji su podaci bili predmet povrede osobnih podataka o povredi osobnih podataka, sukladno obvezi iz članka 34. stavak 1. Opće uredbe o zaštiti podataka.
5. Za kršenja obveza iz članaka 13., 32., 33. i 34. stavak 1. Opće uredbe o zaštiti podataka, opisana u točkama 1. - 4. izreke ovog rješenja, u skladu s odredbama članka 83. Opće uredbe o zaštiti podataka, izriče se ustanovi Bolnica X iz __, upravna novčana kazna u iznosu od:

3.000,00 Eura
(slovima: tri tisuće eura)
6. Ustanova Bolnica X iz __ 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: __s naznakom – “upravne novčane kazne koje izriče AZOP”.

7. Ukoliko ustanova Bolnica X iz __, u roku od 15 dana od pravomoćnosti ovog rješenja ne plati izrečenu upravnu novčanu kaznu, Agencija za zaštitu osobnih podataka 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.
8. Ustanova Bolnica X iz __ dužna je u roku od 15 dana od izvršene uplate dostaviti dokaz o uplati Agenciji za zaštitu osobnih podataka.

O b r a z l o ž e n j e

I. UTVRĐENJE POVREDE

Dana 11.09.2024. u postupku KLASA: __ pokrenutom protiv Bolnice X (dalje: voditelj obrade), a po zahtjevu za utvrđivanje povrede prava ispitanika čiji su osobni podaci bili predmet povrede osobnih podataka, Agencija za zaštitu osobnih podataka (dalje: Agencija) provela je nadzorno postupanje vezano za usklađenost voditelja obrade sa odredbama Opće uredbe o zaštiti podataka vezano za transparentnost i sigurnost obrade osobnih podataka. Rješenjem KLASA: __, URBROJ: __ od __ utvrđeno je kako je povreda osobnih podataka (dalje: predmetna povreda osobnih podataka) nastala kao posljedica kršenja sigurnosti koje je dovelo do neovlaštenog otkrivanja medicinske dokumentacije medijima, pohranjene u bolničkom informacijskom sustavu predmetnog voditelja obrade. Važno je istaknuti kako je u predmetnoj situaciji nepoznati zaposlenik voditelja obrade fotografirao zaslon računala na kojem se nalazio prikaz medicinskog nalaza sa sadržanim podacima pacijenata. Tijekom provedbe nadzornog postupanja utvrđene su nepravilnosti koje nisu bile predmet zahtjeva ispitanika temeljem čijeg zahtjeva je pokrenut postupak, slijedom navedenog pokrenut je i postupak po službenoj dužnosti, poradi usklađivanja postupaka obrade osobnih podataka sa odredbama Opće uredbe o zaštiti podataka.

U tijeku postupka Agencija je dana 11.09.2024. godine izvršila izravne nadzorne aktivnosti kod voditelja obrade Bolnice X, a o čemu je sastavljen Zapisnik o provedenom nadzoru od 11.09.2024. godine (KLASA: __; URBROJ: __ koji prileži spisu predmeta).

Predmetnim nadzornim postupanjem utvrđeno je kako voditelj obrade nije na transparentan način ispitanicima pružio informacije o obradi osobnih podataka. Naime, do dana provedbe nadzora na web stranicama voditelja obrade ispitanicima su bile pružene informacije u vidu odluke o imenovanju Službenika za zaštitu osobnih podataka, kontakt podaci i predložak obrasca za ostvarivanje prava, a zasebni akt odnosan na informacije o obradi osobnih podataka nije bio sačinjen, isto je utvrđeno tijekom nadzornog postupanja sukladno izjavi službenika za zaštitu osobnih podataka imenovanog od strane voditelja obrade (dalje: službenik za zaštitu osobnih podataka).

Nakon provedenog nadzora, Agencija je aktom KLASA: __, URBROJ: __ od 17.09.2024. još jednom zatražila od voditelja obrade da se očituje o načinu informiranja ispitanika o obradi osobnih podataka. Dana 01.10.2024. Agencija je zaprimila traženo očitovanje voditelja obrade

u kojem se navodi kako je voditelj obrade nakon provedenog nadzora na web stranicama objavio informacije o obradi osobnih podataka u zasebnom dokumentu.

U odnosu na upit službenika Agencije, postavljenog tijekom nadzora na dan 11.09.2024., da li su donesene izmjene i dopune internog akta naziva „Pravilnika o prikupljanju, obradi i zaštiti osobnih podataka Bolnice X“ od 27.09.2018. godine te da li postoje drugi akti odnosni na zaštitu osobnih podataka i primjenu organizacijsko-tehničkih mjera zaštite, službenica za zaštitu osobnih podataka navela je kako je navedeni Pravilnik aktualan te da je još donesen interni akt Sigurnosna procedura i dodatak iste. Također, službenica za zaštitu osobnih podataka tijekom nadzora priložila je i dokument naziva „Zaštita osobnih podataka - uputa“.

Uvidom u interni akt voditelja obrade naziva „Pravilnika o prikupljanju, obradi i zaštiti osobnih podataka Bolnice X“ od 27.09.2018. (dalje: Pravilnik) utvrđeno je kako isti ne definira pojam povrede osobnih podataka. Nadalje, čl. 13. Pravilnika propisano je kako su voditelji organizacijskih jedinica dužni o povredi osobnih podataka obavijestiti Službenika za zaštitu osobnih podataka. Člankom 20. Pravilnika, između ostalog, propisano je kako voditelj obrade provodi mjere zaštite osobnih podataka na način da ovlaštene osobe za obradu osobnih podataka odgovorne za zaštitu osobnih podataka od slučajnog ili nezakonitog uništenja, gubitka, izmjene i neovlaštenog pristupa, bez definiranja ovlaštenih osoba za obradu osobnih podataka kao ni načina na koji bi isto trebali učiniti.

Uvidom u interni akt voditelja obrade naziva „Procedura informacijskog sustava Bolnice X“ od 28.02.2022. godine (dalje: Procedura) utvrđeno je kako u toč. IX. Procedure propisano je kako nije dozvoljeno unošenje privatne računalne i komunikacijske opreme i njezino povezivanje na informatički sustav ustanove. Nadalje, istom točkom propisano je kao je korisnik dužan gubitak računalnih i komunikacijski uređaja dužan prijaviti Odsjeku za informatiku.

Uvidom u dokument naziva „Zaštita osobnih podataka - uputa“ (dalje: Uputa) utvrđeno je kako isti, između ostalog, sadrži i slijedeću uputu: „U slučaju povrede osobnih podataka, a koje su vezane na naš sustav obrade istih, dužni smo obavijestiti sve relevantne osobe te nadležno tijelo u roku od 72 sata od saznanja o povredi i to ako je vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinca.“

Tijekom nadzora koji je proveden 11.09.2024. na upit ovlaštenog službenika Agencije, kada i na koji način je voditelj obrade saznao za predmetnu povredu osobnih podataka u vidu, objave fotografije zaslona računala na kojoj je vidljiv medicinski nalaz ispitanika u medijima, predstavnik voditelja obrade naveo je kako su informacije o navedenom događaju bile svima vidljive iz objave u medijima te da mu nije poznat točan datum te da je odmah, 16.11.2023., po dojavi u medijima o iznošenju tih podataka postupanje započela i policija. Nadalje na upit u odnosu na razlog ne izvještavanja nadzornog tijela (Agencije) u zakonskom roku od 72 sata predstavnik voditelja obrade naveo je kako je inicijalnom provjerom utvrđeno da nije bilo upada u sustav pohrane bolnice, već da se radi o postupanju nekog od zaposlenika, a što predstavlja kazneno djelo, a čije je rješavanje u nadležnosti policije. Slijedom navedenog, predstavnik voditelja obrade naveo je kako su smatrali da nije potrebno izvještavati Agenciju kao nadzorno tijelo za provedbu Opće uredbe o zaštiti podataka. Nadalje, u odnosu na pitanje iz kojeg razloga voditelji organizacijskih jedinica unutar kojih je došlo do povrede osobnih podataka nisu o povredi izvijestili službenika za zaštitu osobnih podataka imenovanog od strane voditelja obrade, predstavnik voditelja obrade naveo je kako nakon započetog

postupanja od strane policije, nisu iz opreza uključivali širi krug ljudi osim direktno odgovornih obzirom da su izvidi policije tajni.

Tijekom nadzora koji je proveden 11.09.2024. na upit ovlaštenog službenika Agencije, da li je po saznanju o događaju u vidu iznošenja zdravstvenih podataka iz sustava pohrane voditelja obrade poslana kakva informacija ispitaniku čiji su podaci bili neovlašteno dostavljeni medijima, službenica za zaštitu osobnih podataka imenovana od voditelja obrade navela je kako su ispitaniku pružene informacije vezane za povredu osobnih podataka tek nakon što se ispitanikov punomoćnik obratio voditelju obrade. Na izravan upit da li sačinjena analiza u odnosu na mogućnost nastupa rizika za prava i slobode pojedinca sukladno članku 34. Opće uredbe o zaštiti podataka službenica za zaštitu osobnih podataka navela je kako isto nije učinjeno te da je ona kao službenik za zaštitu podataka uključena u rješidbu konkretne problematike tek po zaprimanju dopisa ispitanikovog punomoćnika obzirom na okolnost provođenja izvida od strane policije zbog počinjenja kaznenog djela, iz kojeg razloga se smatralo da nije potrebno poduzimati druge mjere i radnje.

Nastavno na navedeno, ističemo kako se od 25. svibnja 2018., u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, izravno i obvezujuće primjenjuje Opća uredba o zaštiti podataka.

Člankom 4. pod toč. 12. propisano je: “ „povreda osobnih podataka” znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;“

Člankom 13. Opće uredbe o zaštiti podataka propisano je:

„1. Ako su osobni podaci koji se odnose na ispitanika prikupljeni od ispitanika, voditelj obrade u trenutku prikupljanja osobnih podataka ispitaniku pruža sve sljedeće informacije:

- (a) identitet i kontaktne podatke voditelja obrade i, ako je primjenjivo, predstavnika voditelja obrade;
- (b) kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;
- (c) svrhe obrade radi kojih se upotrebljavaju osobni podaci kao i pravnu osnovu za obradu;
- (d) ako se obrada temelji na članku 6. stavku 1. točki (f), legitimne interese voditelja obrade ili treće strane;
- (e) primatelje ili kategorije primatelja osobnih podataka, ako ih ima; i
- (f) ako je primjenjivo, činjenicu da voditelj obrade namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji te postojanje ili nepostojanje odluke Komisije o primjerenosti, ili u slučaju prijenosa iz članaka 46. ili 47. ili članka 49. stavka 1. drugog podstavka upućivanje na prikladne ili odgovarajuće zaštitne mjere i načine pribavljanja njihove kopije ili mjesta na kojem su stavljene na raspolaganje.

2. Osim informacija iz stavka 1., voditelj obrade u trenutku kada se osobni podaci prikupljaju pruža ispitaniku sljedeće dodatne informacije potrebne kako bi se osigurala poštena i transparentna obrada:

- (a) razdoblje u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje;
- (b) postojanje prava da se od voditelja obrade zatraži pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade koji se odnose na ispitanika ili prava na ulaganje prigovora na obradu takvih te prava na prenosivost podataka;
- (c) ako se obrada temelji na članku 6. stavku 1. točki (a) ili članku 9. stavku 2. točki (a), postojanje prava da se u bilo kojem trenutku povuče privolu, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena;
- (d) pravo na podnošenje prigovora nadzornom tijelu;

- (e) informaciju o tome je li 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;
 - (f) postojanje automatiziranog donošenja odluka, što uključuje izradu profila iz članka 22. stavaka 1. i 4. te, barem u tim slučajevima, smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za ispitanika.
3. Ako voditelj obrade namjerava dodatno obrađivati osobne podatke u svrhu koja je različita od one za koju su osobni podaci prikupljeni, voditelj obrade prije te dodatne obrade ispitaniku pruža informacije o toj drugoj svrsi te sve druge relevantne informacije iz stavka 2.
4. Stavci 1., 2. i 3. ne primjenjuju se ako i u onoj mjeri u kojoj ispitanik već raspolaze informacijama.“

Člankom 32. Opće uredbe o zaštiti podataka propisano je:

„1. 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:

- (a) pseudonimizaciju i enkripciju osobnih podataka;
 - (b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;
 - (c) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;
 - (d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.
2. Prilikom procjene odgovarajuće razine sigurnosti u obzir se 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.
3. Poštovanje odobrenog kodeksa ponašanja iz članka 40. ili odobrenog mehanizma certificiranja iz članka 42. može se iskoristiti kao element za dokazivanje sukladnosti sa zahtjevima iz stavka 1. ovog članka.
4. Voditelj obrade i izvršitelj obrade poduzimaju mjere kako bi osigurali da svaki pojedinac koji djeluje pod odgovornošću voditelja obrade ili izvršitelja obrade, a koji ima pristup osobnim podacima, ne obrađuje te podatke ako to nije prema uputama voditelja obrade, osim ako je to obavezan učiniti prema pravu Unije ili pravu države članice.“

Člankom 33. Opće uredbe o zaštiti podataka propisano je:

- „1. 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.
2. Izvršitelj obrade bez nepotrebnog odgađanja izvješćuje voditelja obrade nakon što sazna za povredu osobnih podataka.
3. U izvješćivanju iz stavka 1. mora se barem:
- (a) opisati priroda povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;
 - (b) navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;

- (c) opisati vjerojatne posljedice povrede osobnih podataka;
 - (d) opisati mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.
4. Ako i u ovoj mjeri u kojoj nije moguće istodobno pružiti informacije, informacije je moguće postupno pružiti bez nepotrebnog daljnjeg odgađanja.
5. Voditelj obrade dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljivanje štete. Ta dokumentacija nadzornom tijelu omogućuje provjeru poštovanja ovog članka.“

Člankom 34. Opće uredbe o zaštiti podataka propisano je:

- „1. U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.
2. Obavješćivanjem ispitanika iz stavka 1. ovog članka opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava barem informacije i mjere iz članka 33. stavka 3. točaka (b), (c) i (d).
3. Obavješćivanje ispitanika iz stavka 1. nije obvezno ako je ispunjen bilo koji od sljedećih uvjeta:
- (a) voditelj obrade poduzeo je odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija;
 - (b) voditelj obrade poduzeo je naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika iz stavka 1.;
 - (c) time bi se zahtijevao nerazmjern napor. U takvom slučaju mora postojati javno obavješćivanje ili slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način.
4. Ako voditelj obrade nije do tog trenutka obavijestio ispitanika o povredi osobnih podataka, nakon razmatranja razine vjerojatnosti da će povreda osobnih podataka prouzročiti visok rizik, nadzorno tijelo može od njega zahtijevati da to učini ili može zaključiti da je ispunjen neki od uvjeta navedenih u stavku 3.“

Slijedom navedenog, u ovoj upravnoj stvari utvrđeno je kako voditelj obrade u razdoblju od 25.05.2018. do rujna 2024. godine nije ispitanicima pružio osnovne informacije o obradi osobnih podataka u vidu informacija; o svrhama obrade radi kojih se upotrebljavaju osobni podaci kao i pravnim osnovama za obradu; legitimnim interesima voditelja obrade ili treće strane; primateljima ili kategorijama primatelja osobnih podataka, kao ni informacije o; razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje te informacije o tome je li 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. Temeljem čega je utvrđeno kršenje članka 13. Opće uredbe o zaštiti podataka.

Tijekom ovog upravnog postupka uvidom u interne akte Pravilnik, Procedura i Uputa te izjave predstavnika voditelja obrade dane tijekom provedenog nadzora od 11.09.2024. utvrđeno je kako voditelj obrade ne raspoznaje situacije i događaje koje predstavljaju moguću povredu osobnih podataka i koje mogu negativno utjecati na prava i slobode pojedinaca. Naime, u konkretnom slučaju voditelj obrade događaj u vidu neovlaštenog otkrivanja osobnih podataka ispitanika koji su pohranjeni u bolničkom informacijskom sustavu nije prepoznao kao povredu osobnih podataka, već je predmetni događaj definirao samo kao kazneno djelo nedozvoljene

uporabe osobnih podataka iz čl. 146. Kaznenog zakona. Nadalje, isto proizlazi i iz internog akta Procedura kojim je propisano kako je korisnik dužan gubitak računalnih i komunikacijski uređaja dužan prijaviti Odsjeku za informatiku, no ne i Službeniku za zaštitu podataka, koji pravovremeno mora biti upoznat o povredi osobnih podataka. Ovdje je bitno istaknuti kako i Kazneni zakon u Glavi dvadeset pet, definira niz kaznenih djela protiv računalnih sustava, programa i podataka, primjerice; neovlašteni pristup računalnim sustavima ili nekom njegovom dijelu ili računalnim podacima; neovlaštena oštećenje, izmjena, brisanje, uništenje ili prikrivanje tuđih računalnih podataka ili programa ili onemogućavanje pristupa tuđim računalnim podacima ili programima, a koji se vrlo često mogu rezultirati povredom osobnih podataka u vidu uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima. U navedenim situacijama kaznenu odgovornost snosi počinitelj kaznenog djela, ali i u smislu odredbi Opće uredbe o zaštiti podataka potencijalno i voditelj obrade ukoliko nije implementirao odgovarajuće tehničke i organizacijske mjere kako bi sveo rizik od povrede osobnih podataka na najmanju moguću razinu.

Nadalje, vezano za kršenje sigurnosti obrade osobnih podataka utvrđeno je kako internim aktima nije propisan način na koji će službenik za zaštitu osobnih podataka provoditi kontrolu i nadzor nad procesima obrade osobnih podataka. Također, utvrđeno je kako interni akti nisu revidirani od njihovog donošenja. Naime, Pravilnik nije revidiran od 2018. godine, dok Procedura nije revidirana od 2022. godine, unatoč tome što je jedna od obveza voditelja obrade da redovno testira, ocjenjuje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Također, na nerazumijevanje obveza voditelja obrade po Općoj uredbi o zaštiti podataka govori i odredba čl. 20. Pravilnika kojom je, između ostalog, propisano kako voditelj obrade provodi mjere zaštite osobnih podataka na način da su ovlaštene osobe za obradu osobnih podataka odgovorne za zaštitu osobnih podataka od slučajnog ili nezakonitog uništenja, gubitka, izmjene i neovlaštenog pristupa. Naime, upravo je voditelj obrade kao ustanova odgovoran za sigurnost obrade osobnih podataka u vidu implementiranja odgovarajućih tehničkih i organizacijskih mjera koje imaju za cilj da ne dođe do kršenja sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani, a ne ovlaštene osobe za obradu. Naime, sukladno odredbama članka 32. Opće uredbe o zaštiti podataka voditelj obrade odgovoran je za poduzimanje mjera kako bi osigurao da svaki pojedinac koji djeluje pod njegovom odgovornošću, a koji ima pristup osobnim podacima, ne obrađuje te podatke ako to nije prema uputama voditelja obrade.

Uvidom u sve dostavljene dokumente od strane voditelja obrade, proizlazi da voditelj obrade ne razlikuje povredu prava ispitanika od povrede osobnih podataka. Nadalje, Pravilnikom, kao ni drugim aktima nije propisano na koji način se procjenjuje da li će povreda osobnih podataka prouzročiti visok rizik za prava i slobode pojedinaca. Pravilnikom nije propisan način na koji će službenik za zaštitu osobnih podataka provoditi kontrolu i nadzor nad procesima obrade osobnih podataka.

Dakle, voditelj obrade ima obvezu sukladno Općoj uredbi o zaštiti podataka internim aktima detaljno propisati način obrade osobnih podataka, a kako bi bio u mogućnosti dokazati kako je poduzeo mjere kako bi osigurao da svaki pojedinac koji djeluje pod njegovom odgovornošću, obrađuje podatke prema uputama. U konkretnom slučaju voditelj obrade je Agenciji dostavio interne akte koji nisu u dovoljnoj mjeri razrađeni, odnosno u istima nisu sadržane jasne upute o načinu postupanja zaposlenika/ osoba pod odgovornošću voditelja obrade kod obrade osobnih podataka.

Naime, od bolnice kao voditelja visoko rizične obrade posebne kategorije osobnih podataka o zdravlju očekuje se da sukladno visokom riziku detaljno razradi organizacijske mjere. Primjerice ista bi trebala imati razrađene interne akte u vidu pravilnika koji definira sve aspekte zaštite osobnih podataka pacijenata i zaposlenika, uključujući pravila o prikupljanju, obradi, pohrani i pristupu osobnim podacima, regulira prava ispitanika (pacijenata), poput prava na pristup, ispravak i brisanje podataka, procedure za ostvarivanje prava pacijenata na pristup njihovim podacima, ispravak, prijenos i brisanje podataka, kao i proceduru za upravljanje pritužbama i prigovorima vezanim uz obradu njihovih osobnih podataka kao i obvezu obavještanja o povredama podataka, a kojim su jasno definirane odgovorne osobe. Nadalje, obzirom na to da bolnice često čuvaju osjetljive medicinske podatke, voditelj obrade treba razraditi interni pravilnik o zadržavanju podataka kojim se definirati koliko dugo će podaci biti pohranjeni (na temelju zakonskih rokova) i način njihovog sigurnog brisanja kad istekne rok ili kada podaci više nisu potrebni za svrhu obrade, kao i odgovornih osoba za navedeno. Također, neophodan je i pravilnik o informacijskoj sigurnosti kojim se propisuju mjere zaštite informacija unutar bolnice, što uključuje sigurnost IT sustava, zaštitu od cyber prijetnji, enkripciju podataka, sigurnost mreža, antivirusnu zaštitu i upravljanje pristupom osjetljivim podacima. Nadalje, važan je pravilnik koji propisuje tehničke mjere za sigurnost računalnih sustava i mreža. To uključuje pravila o vatrozidu, šifriranju podataka u prijenosu, sigurnosnim kopijama podataka (backup), te o zaštiti od neovlaštenog pristupa. Također, potrebno je definirati i pristupne kontrole i nadzor, uključujući upotrebu kartica za pristup, video nadzor i ograničavanje pristupa određenim područjima. Također, internim aktima treba osigurati da samo ovlašteni zaposlenici imaju pristup osjetljivim podacima pacijenata i drugih važnih informacija unutar bolnice. To uključuje definiranje prava pristupa, pravila za kreiranje i opoziv lozinki, te kontrolu privilegija pristupa na temelju pozicije i odgovornosti zaposlenika. Internim pravilnicima treba propisati i redovite obuke i testove za osoblje, kako bi bili upoznati s najboljim praksama zaštite podataka, prepoznavanjem sigurnosnih prijetnji i odgovornostima vezanim uz obradu podataka. Nadalje, internim pravilnicima regulira se i postupanje u slučaju sigurnosnog incidenta, kao što je cyber napad, neovlašteni pristup podacima ili gubitak podataka. Propisuje protokole za prijavu incidenata, njihovu analizu i obavještanje nadležnih tijela.

Bolnica kao voditelj obrade mora osigurati da svi zaposlenici, od medicinskog osoblja do administrativnog, budu upoznati sa organizacijskim i tehničkim mjerama te da ih dosljedno primjenjuju kako bi osigurali sigurnost podataka i zaštitu prava ispitanika/ pacijenata.

Slijedom navedenog, a obzirom na to da je tijekom ovog postupka utvrđeno kako su organizacijske mjere sadržane u dostavljenim internim aktima voditelja obrade ne adekvatne, neažurne odnosno ne odgovaraju riziku obrade utvrđeno je kršenje čl. 32. Opće uredbe o zaštiti podataka.

Kršenje članka 33. Opće uredbe o zaštiti podataka utvrđeno je obzirom da voditelj obrade nije u zakonskom roku od 72 sata od saznanja za povredu osobnih podataka izvijestio Agenciju za zaštitu osobnih podataka kao nadzorno tijelo o povredi osobnih podataka u vidu objave u medijima fotografije sa prikazom zaslona na kojem su prikazani medicinski podaci ispitanika/pacijenta sadržani unutar BIS-a bolnice iako je o istom saznanja imao 16.11.2023. te činjenice da voditelj obrade nije dokumentirao niti jednu povredu osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljivanje štete u razdoblju od 6 godina.

Zaključno, utvrđeno je kršenje članka 34. st. 1. Opće uredbe o zaštiti podataka obzirom da je utvrđeno kako voditelj obrade u konkretnom slučaju nije obavijestio ispitanika o povredi osobnih podataka iako je imao saznanja da su njegovi zdravstveni podaci neovlašteno otkriveni medijima.

II. UTVRĐENJE UPRAVNE NOVČANE KAZNE

Člankom 44. Zakona o provedbi Opće uredbe o zaštiti podataka 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.

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 dospelju 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 dospelju, 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 upravno 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. 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 i/ili izvršitelju 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 upravno 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 vezano za sigurnost obrade osobnih podataka te postupanja u slučaju povrede osobnih podataka. 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 istih 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.

Nadalje, odredba stavaka 3. istog članka propisuje ako voditelj obrade ili izvršitelj obrade za istu ili povezane obrade namjerno ili iz nepažnje prekrši nekoliko odredaba ove Uredbe ukupan iznos novčane kazne ne smije biti veći od administrativnog iznosa utvrđenog za najteže kršenje. U članku 83. stavku 4. Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade propisanih člancima 32., 33. i 34. Opće uredbe o zaštiti podataka mogu izreći upravne novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.

U članku 83. stavku 5. Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade propisanih člankom 13. 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.

Agencija je radi kršenja članaka 13., 32., 33. i 34. Opće uredbe o zaštiti osobnih podataka izrekla voditelju obrade Bolnici X upravnu novčanu kaznu u iznosu od 3.000,00 EUR.

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, utvrđeno je kako je voditelj obrade Bolnica X i 6 godina nakon stupanja na snagu Opće uredbe o zaštiti podataka unatoč visoko rizičnoj i opsežnoj obradi zdravstvenih podataka, kao osnovnoj djelatnosti, nije na odogovarajući način implemetirala organizacijske mjere zaštite u svezi postupanja po povredi osobnih podataka. Zaštita osobnih podataka pacijenta i čuvanje povjerljivosti informacija o zdravlju važno je ne samo radi poštovanja

privatnosti pacijenta, već i radi povjerenja u medicinsku struku i zdravstvene usluge koje pružaju liječnici i drugo medicinsko osoblje.

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

U predmetnom slučaju nije utvrđena izravna namjera kršenja odredaba Opće uredbe o zaštiti podataka od strane voditelja obrade, već je riječ o nemarnom postupanju voditelja obrade.

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

Obzirom da u predmetnom slučaju nije utvrđeno da su ispitanici pretrpjeli štetu ista okolnost nije cijenjena ni kao olakotna ni kao otegotna.

- 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);

Kao otegotnu okolnost Agencija je prilikom izricanja upravno novčane kazne posebno cijenila stupanj nerazumijevanja svojih obveza vezanih za sigurnost obrade posebne kategorije osobnih podataka. Ne postupanjem po obvezama evidentiranja povreda osobnih podataka, neanaliziranjem rizika te neobaviještavanjem nadzornog tijela o povredama osobnih podataka voditelj obrade ozbiljno ugrožava prava i slobode ispitanika čije osobne podatke obrađuje. Također, treba istaknuti kako upravo povrede osobnih podataka služe kao indikatori slabih točaka sustava koje treba unaprijediti kako se iste povrede ne bi opetovano događale, pa je navedeno uzeto u obzir kod visine kazne.

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

Agencija nema evidentirana relevantna prijašnja kršenja odredaba o zaštiti podataka od strane voditelja obrade.

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

Voditelj obrade je tijekom ovog upravnog postupka na odgovarajući način odgovarao na zahtjeve nadzornog tijela.

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

Predmetna okolnost uzeta je u obzir kao otegotna obzirom da je voditelju obrade osnovna djelatnost upravo obrada zdravstvenih podataka, kao posebne kategorije osobnih podataka iz članka 9. Opće uredbe o zaštiti podataka.

- 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 o povredi osobnih podataka doznala iz zaprimljenog zahtjeva ispitanika, no obzirom da je voditelju obrade izrečena upravno novčana kazna poradi kršenja obveza izvješćivanja nadzornog tijela ista okolnost nije uzeta u obzir prilikom odmjeravanja 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);

Obzirom da voditelju obrade nije prethodno izrečena mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka, predmetna okolnost nije uzeta u obzir prilikom određivanja iznosa upravno novčane kazne.

- 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 relevantno.

- 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);

Prilikom određivanja iznosa upravne novčane kazne Agencija nije utvrdila druge relevantne okolnosti koje bi se imale smatrati otegotnima ili olakotnim.

Novčana kazna može se smatrati učinkovitom ako se njome postižu ciljevi zbog kojih je izrečena. To može biti ponovna uspostava poštivanja pravila, kažnjavanje nezakonitog ponašanja ili oboje. Agencija se odlučila upravo za izricanje upravne novčane kazne kao korektivne mjere iz razloga što voditelj obrade ni nakon 6 godina od početka primjene Opće uredbe o zaštiti podataka, unatoč činjenici da obrađuje zdravstvene podatke kao posebnu kategoriju osobnih podataka ne raspoznaje svoje obveze iz Opće uredbe o zaštiti podataka kao ni povrede osobnih podataka. Naime jedno od osnovnih načela obrade osobnih podataka je obveza voditelja obrade da obrada osobnih podataka bude sigurna, odnosno da implementira odgovarajuće organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti uzimajući u obzir rizik za prava i slobode pojedinaca. Činjenica da povrede osobnih podataka u bolnicama mogu uzrokovati visok rizik za prava i slobode pa čak u vidu i smrtnih posljedica je od odlučne važnosti. Voditelj obrade u konkretnom slučaju ne može osigurati odgovarajuću razinu sigurnosti ukoliko ne raspoznaje povrede osobnih podataka, ne uključuje službenika za zaštitu osobnih podataka u pitanja vezana za zaštitu osobnih podataka te ne provodi redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti organizacijskih mjera za osiguravanje sigurnosti obrade.

Agencija je provela ispitni postupak sukladno člancima 51. i 52. Zakona o općem upravnom postupku i sukladno svim načelima upravnog postupka propisanih ZUP-om, pravilno utvrdila činjenično stanje te je na temelju utvrđenog činjeničnog stanja pravilno primijenila materijalno pravo i izvela pravilan zaključak o činjeničnom stanju u konkretnom predmetu. Svoju odluku temelji na svim relevantnim dokazima i činjenicama kojima je raspolagala i koje je voditelj obrade dostavio kao dokaze.

Jednako tako, uzimajući u obzir sve prethodno navedeno Agencija smatra da je upravo korektivna mjera u vidu upravne novčane kazne učinkovita, proporcionalna i odvrćajuća u ovoj upravnoj stvari, te da je njezin iznos u potpunosti primjeren okolnostima konkretnog slučaja.

Temeljem svega navedenog odlučeno je kao u Izreci Rješenja.

UPUTA O PRAVNOM LIJEKU

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

RAVNATELJ

Zdravko Vukić, univ. mag. oec.

DOSTAVITI:

1. Bolnica X,
2. Pismohrana, ovdje