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, članaka 36., 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18), a postupajući po službenoj dužnosti protiv voditelja obrade Bolnice X, radi zaštite osobnih podataka, donosi sljedeće:

R J E Š E NJ E

1. Utvrđuje se da je nepoduzimanjem odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka od strane voditelja obrade Bolnice X, odnosno postupanjem protivno članku 32. stavku 1. točke b) i d) te stavku 2. Opće uredbe o zaštiti podataka, došlo do kršenja sigurnosti koje je dovelo neovlaštenog pristupa osobnim podacima ispitanika.

2. Za kršenje opisano u točki 1. izreke ovog rješenja, u skladu s odredbama članka 83. stavka 2. i stavka 4. točke a) Opće uredbe o zaštiti podataka, izriče se voditelju obrade Bolnici X, upravna novčana kazna u iznosu od:

20.000,00 EUR
(slovima: dvadesettisućaeura)

3. Voditelj obrade Bolnica X 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”.

4. Ukoliko voditelj obrade Bolnica X, 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.

5. Voditelj obrade Bolnica X, 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 nj e

I. UTVRĐENJE POVREDE

Agencija za zaštitu osobnih podataka (dalje u tekstu: Agencija) se dopisom KLASA:, URBROJ: obratila voditelju obrade Bolnici X, (dalje u tekstu: Bolnica X) nastavno na objave u medijima iz kojih je bilo razvidno da je unutar sustava voditelja obrade Bolnice X došlo do sigurnosnog incidenta povezanog s kibernetičkim napadom, a posredno time i do ugroze osobnih podataka ispitanika koje predmetni voditelj obrade obrađuje te zatražila žurno dostavu informacija da li je i u kojem opsegu došlo do povrede/ugroze osobnih podataka kao i koje povrede (nedostupnost privremena, kriptiranje, iznošenje, gubitak), navođenje koji sustavi pohrane su zahvaćeni, koje su kategorije ispitanika zahvaćene i koji opseg osobnih podataka (identifikacijski, podaci o zdravlju, medicinska dokumentacija) i ukupan broj ispitanika. Istim dopisom zatražena je dostava informacija i relevantna dokumentacija u svezi primjenjivanih tehničkih i organizacijskih mjera zaštite osobnih podataka kao i internih akata odnosnih na zaštitu osobnih podataka.

Agencija je zaprimila od voditelja obrade Bolnice X Izvješće o povredi osobnih podataka sukladno članku 33. stavku 1. Opće uredbe o zaštiti podataka u kojem se u bitnome navodi da je povreda osobnih podataka koja je zadesila Bolnicu X posljedica ransomware (Lockbit 3.0) napada koji se dogodio u ranim jutarnjim satima, da su kriptirana dva od tri domenska kontrolera, kriptiran dio sadržaja na backup serveru te sadržaj radiološkog informacijskog sustava, da Bolnički informacijski sustav udomljen u CDU nije zahvaćen incidentom, da je o incidentu obaviješten MUP, ZSIS i SOA te da su u suradnji s navedenim tijelima u tijeku istražne radnje.

Agencija je zaprimila dodatno očitovanje Bolnice X kojim se navodi da su nastavno na predmetnu povredu u međuvremenu sukcesivno funkcionalno uspostavljeni veći dijelovi sustava koji su od trenutka saznanja za incident bili isključeni radi preventivnih mjera provedenih u svrhu sigurnosne provjere te se navodi da su pored organizacijskih mjera do sada u Bolnici X implementirane tehničke mjere i rješenja i to: osiguranje perimetra računalne mreže i mrežnog prometa putem vatrozida (Firewalla), segmentacija računalne mreže u VLAN-ove,

VPN pristup za udaljeni rad i spajanje na mrežu, antivirusna zaštita računala i servera, rješenje za prevenciju upada u računalnu mrežu (IPS), rješenje za detekciju malicioznog ponašanja na mreži (NDR) i rješenje za upravljanje i nadzor privilegiranim korisničkim računima (PAM). Dalje se navodi da su u odnosu na korištenje bolničkog informacijskog sustava usvojeni interni akti i to, Sustav upravljanja sigurnošću: Pravila o odabiru i korištenju lozinki, Sustav upravljanja sigurnošću: Upravljanje pristupnim pravima BIPSI, Medicinska dokumentacija: Pravo pristupa i povjerljivost medicinske dokumentacije vođene u elektroničkom obliku i bolničkom informacijskom sustavu, Sustav upravljanja sigurnošću: Upravljanje pristupom računalnoj mreži Bolnice X, Bolnički i poslovni sustav informacija: Uputa za promjenu lozinke domenskog korisničkog računa, Informacijski sustav Bolnice X: Kreiranje, izmjene i korištenje lozinki za pristup računalnoj mreži i pripadajućim servisima, Popunjavanje i pronalaženje medicinskih kartona, Informacijski sustav Bolnice X: Zahtjev za aktivacijom korisničkog računa za pristup računalnim servisima Bolnice X, Zahtjev za dodjelu i izmjenu korisničkih prava. Dalje se navodi da su organizacijske mjere zaštite propisane internim aktima; Pravilnikom o medicinskoj dokumentaciji, Pravilnikom za upravljanje dokumentiranim gradivom, Pravilnikom o profesionalnoj tajni, te da je osim navedenog Bolnica X donio Pravilnik o prikupljanju, obradi i zaštiti osobnih podataka i Politiku o zaštiti osobnih podataka i privatnosti s pripadajućim obrascima (Izjava o povjerljivosti, Zahtjev za pristup osobnim podacima, Zahtjev za ispravak ili dopuna osobnih podataka, Zahtjev za brisanje osobnih podataka, Zahtjev za ograničenje obrade osobnih podataka, Zahtjev za prenosivost osobnih podataka, Prigovor na obradu osobnih podataka).
Očitovanju se prilaže *Obrazac prijelaznog izvješća o incidentu sa znatnim učinkom* koji između ostalog navodi da je Lockbit 3.0, prema trenutnim saznanjima, inicijalni ulaz ostvario preko kompromitiranog VPN računa običnog korisnika putem kojeg je uspio doći do kredencijala domenskog administratora jednog servisnog računa, da su kriptirani sustavi.

Agencija je zaprimila dodatne informacije u pisanom obliku voditelja obrade Bolnice X kojima se navode serveri koji su zahvaćeni predmetnom povredom i kriptirani od strane napadača.

Agencija je provela nadzor kod voditelja obrade Bolnice X o čemu je sačinjen Zapisnik o provedenom nadzoru KLASA:, URBROJ:, kojim je utvrđeno (provedenim istražnim radnjama) da je prvo neovlašteno spajanje putem VPN-a zabilježeno 2024. korištenjem legitimnog korisničkog računa s rumunjske IP adrese, da kada je napadač ušao u mrežu korištenjem računa iskoristio je slabost sustava i zadobio domain admin ovlasti, da točnu ranjivost nije moguće utvrditi, da je napadač na domenski kontroler prenio izvršnu datoteku (.exe) za skeniranje mreže te započeo skeniranje iste i dovršio, da je napadač zatim instalirao program za kopiranje podataka i zakazao početak kopiranja (sheduled task), da je ___2024. bio prvi pokušaj kopiranja ali da je spriječen na firewall-u.

Dalje je utvrđeno da je ukupan broj aktivnih VPN korisničkih računa na dan predmetnog incidenta bio xy internih (zaposlenici) i vanjskih dobavljača/suradnika xy, da Bolnica X ima više back-upova, da je jedan u Centru dijeljenih usluga (CDU) koji navedeni centar održava, da je drugi u Bolnici X lokalno unutar server sobe s tim da su podijeljeni na dio koji održava Bolnica X i drugi koji održavaju vanjski specijalistički dobavljači usluga, da inicijalni podatak

o broju ispitanika zahvaćenih predmetnom povredom od xy naveden u dopuni Izvješća o povredi osobnih podataka je odnosan na ukupan broj ispitanika kojima kompromitirani dijelovi informacijskog sustava nisu bili dostupni te ne predstavlja broj ispitanika čiji su osobnih podaci kompromitirani, da se podaci o pacijentima nalaze u Bolničkom Informacijskom Sustavu (BIS) koji se nalazi na CDU-u i koji nije bio zahvaćen predmetnom povredom, da se svi podaci vezani za zaposlenike nalaze na CDU-u i također nisu bili zahvaćeni predmetnom povredom jer je pristup istima na vrijeme onemogućen.
Predstavnik voditelja obrade je tijekom nadzora izjavio da je File Share koji je bio kompromitiran u predmetnoj povredi namijenjen korisnicima da mogu spremati datoteke koje su im potrebne, da se uglavnom radi o datotekama u ".jpg" i ".pdf" formatu, te da Bolnica X ne može kontrolirati što korisnici spremaju na File Share ali pretpostavlja da spremaju datoteke kao što su npr. znanstveni radovi, CV-evi i slično. Dodatno se pojašnjava da je Bolnica X u trenutku predmetne povrede koristio dva File Share-a, prvi koji je stariji i za koji postoji sumnja da je kompromitiran i da podaci na njemu nisu bili zakriptirani, te drugi noviji na kojem su definirana nova prava, pri čemu se korisnicima na zahtjev prenose podaci sa starog na novi u skladu s poslovnom opravdanošću te se dugoročno planira gašenje prvog File Share-a.

Tijekom nadzora službenici Agencije su proveli uvid u sadržaj prvog File Share-a koji se nalazi unutar sustava pohrane koji je pohranjen u server sobi Bolnice X pri čemu je pristup ostvaren putem konzole od strane administratora i utvrđeno je da se na istome nalaze mape svakog od odjela Bolnice X te dodatno kreirane mape za potrebe zajedničkih poslova zaposlenika, da je uvidom u nasumično odabranu mapu naziva "O" i uvidom u podmape naziva "xy" pronađeno nekoliko datoteka naziva odnosnih na edukacijske materijale ili predavanja.

Daljnjim nasumičnim odabirom mape naziva "K" i uvidom u podmapu naziva "K slike" pronađena je pdf datoteka naziva "xz" na kojoj je skica operativnog zahvata bez vidljivih osobnih podatka.

Dalje, nasumičnim odabirom mape "U" i uvidom u podmapu naziva "Dokumenti" pronađeno je više podmapa s datotekama nekoliko različitih ekstenzija, uvidom u podmapu naziva "xx" pronađena je datoteka "anamneza.doc" koju nije bilo moguće otvoriti jer poslužitelj nema instaliran program za otvaranje navedenog formata ".doc". Daljnjim odabirom mape "z" utvrđeno je da ista sadrži više mapa koje nose nazive imena i prezimena osobe, a koje sadrže dokumente s imenom i prezimenom te adresom stanovanja iste osobe na koju glasi mapa, da je ukupan broj takvih mapa 180. Nasumičnim odabirom mape „aa" utvrđuje se da ista sadrži datoteke „aa" i „aa.x1sx" pri čemu je prva u Word formatu te je nakon uspješnog otvaranja utvrđeno da sadrži ime i prezime imenovanog i njegovu adresu stanovanja, a nasumičnim otvaranjem drugih mapa koje nose nazive imena i prezimena osobe utvrđuje se da iste također sadrže jednu datoteku s imenom i prezimenom iste osobe u Word formatu i drugu datoteku u Excel formatu.

Dalje je proveden uvid u mapu "yy" i utvrđeno da ista sadrži mape "yy-novo", i "R" te više drugih Word, Pdf, Excel i slikovnih datoteka (.jpeg), a daljnjim odabirom datoteke "Podaci n" unutar iste mape, utvrđeno je da navedena datoteka sadrži preslike osobne iskaznice, prednja i stražnja strana, na ime nn i nnn te presliku prednje i stražnje strane Bankovne kartice PBZ-a na ime nn.

Daljnjim odabirom mape L i podmape L, utvrđeno je da ista sadrži datoteke koje nose nazive imena i prezimena osoba i to: te otvaranjem svi prethodno navedenih datoteka utvrđeno je da svaka od njih sadrži nalaz o generičkom testiranju.

Uvidom u podmapu L utvrđeno je da ista sadrži mape naziva "serija uzoraka" i rednog broja od 1 do 58, od broja 59 do 83. nazive "serija nn", redni broj 84. naziva "serija uzorak" , redni broj 85. naziva „serija uzoraka gotovo", „Ažurirani nalazi— stavljeni u BIS", „om", da je otvaranjem broja 59. serija " uzoraka gotovo", utvrđeno da ista sadrži datoteke koje nose nazive imena i prezimena osoba i to: a otvaranjem datoteke aa utvrđuje se da ista sadrži nalaz.
Također tijekom provođenja uvida u File Share utvrđeno je da je operativni sustav istog Windows 2008 R2 Standard.

Nastavno na provedeni nadzor i zatraženo istim, Agencija je zaprimila od voditelja obrade Bolnica X dodatno očitovanje i dokumentaciju i to; *Sustav upravljanja sigurnošću: Pravila o odabiru i korištenju lozinki, Sustav upravljanja sigurnošću: Upravljanje pristupnim pravima BIPSI, Informacijski sustav Bolnice X: Upravljanje pristupnim pravima, Medicinska dokumentacija: Pravo pristupa i povjerljivost medicinske dokumentacije vođene u elektroničkom obliku u bolničkom informacijskom sustavu, Sustav upravljanja sigurnošću: Upravljanje pristupom računalnoj mreži Bolnice X, Bolnički i poslovni sustav informacija: Uputa za promjenu lozinke domenskog korisničkog računa, Informacijski sustav Bolnice X: Kreiranje, izmjene i korištenje lozinki za pristup računalnoj mreži i pripadajućim servisima, Popunjavanje i pronalaženje kartona, Informacijski sustav* Bolnice X*: Zahtjev aktivacije korisničkog računa za pristup računalnim servisima Bolnice X, Zahtjev za dodjelu i izmjenu korisničkih prava, Sustav upravljanja sigurnošću VPN pristup, Informacijski sustav- Upute za instalaciju Fortigate SSL VPN klijenta, Informacijski sustav-Upravljanje mapama i korisničkim pravima na mape, Informacijski sustav-Korištenje osobnih i dodijeljenih mapa na datotečnom poslužitelju*.

Nadalje, utvrđeno je kako je internim dokumentima uređena dodjela razina pristupa podacima tj. djelatnicima su omogućene aktivnosti prema radnom mjestu te se korisniku prava dodjeljuju na temelju poslova koje će raditi u sustavu i na temelju organizacijske jedinice s kojima radi, da se svaka vrsta poslova koja se može izvoditi u informacijskom sustavu grupira u određenu „rolu" koja sadrži potrebna prava korisniku rada, da se svakom korisniku ovisno o vrsti poslova koje radi dodjeljuje određena "rola", a prava u "roli" su ograničena na organizacijske jedinice s kojima korisnik radi, da je propisano da su ovlašteni korisnici obvezni podatke iz medicinske dokumentacije pacijenata čuvati od oštećenja, uništenja, neuporabljivosti te neovlaštenih izmjena, brisanja i pristupanja bazama podataka te čuvati podatke od neovlaštene uporabe u bilo kojem smislu ili davanja podataka na uvid drugim neovlaštenim osobama, da su ovlašteni korisnici obvezni čuvati povjerljivost podataka pacijenata u radu na znanstvenim projektima i znanstvenim publikacijama.

Očitovanju se prilaže *Ugovor za nabavu licenci za vatrozid nove generacije, Ugovor za nabavu usluge obnove i održavanja sustava nadzora nad administratorima najvišeg rizika, Ugovor za nabavu licenci za korištenje softverskih proizvoda i usluga za grupu 1 ESET predmeta nabave, Ugovor za nabavu i implementaciju virtualizacijske infrastrukture, Ugovor za nabavu rješenja za*

nadzor i inspekciju mrežnog prometa, Ugovor o nabavi usluge održavanja rješenja za prevenciju mrežnih upada (IPS), Ugovor za nabavu vatrozida nove generacije, Ugovor za nabavu implementacije rješenja za prevenciju mrežnih upada (IPS), Ugovor o nabavi usluge implementacije sustava nadzora nad administratorima najvišeg rizika.

Očitovanju se prilaže Izvješće o provedenoj analizi incidenta izrađeno od strane društva Y te logička shema informacijskog sustava i verzije operativnih sustava instaliranih na informacijskoj infrastrukturi uz relevantne dokaze, te se navodi da su u Bolnici X implementirane slijedeće tehničke mjere i rješenja: osiguranje perimetra računalne mreže i mrežnog prometa putem vatrozida (Firewalla), segmentacija računalne mreže u VLAN-ove, VPN pristup za udaljeni rad i spajanje na mrežu, antivirusna zaštita računala i servera, rješenje za prevenciju upada u računalnu mrežu (IPS), rješenje za detekciju malicioznog ponašanja na mreži (NDR) i rješenje za upravljanje i nadzor privilegiranim korisničkim računima (PAM).

Agencija se dopisom KLASA, URBROJ: obratila voditelju obrade Bolnici X i zatražila očitovanje je li Bolnica X sukladno članku 34. Opće uredbe o zaštiti podataka izvijestila ispitanike koji su bili zahvaćeni predmetnom povredom a u svezi opisanih utvrđenja navedenih u provedenom nadzoru, te da priloži dokaze koji to potkrjepljuju, te ukoliko nije postupio u svezi odredbi članka 34. Opće uredbe o zaštiti podataka da se očituje o razlozima i priloži dokaze u svezi istog.

Agencija je zaprimila očitovanje voditelja obrade Bolnice X u svezi zatraženog dopisom kojim se u bitnome navodi da je Bolnica X temeljem Zakona o kritičnim infrastrukturama (NN 114/22) određen nacionalnom kritičnom infrastrukturom u sektoru zdravstva, da su neposredno po kibernetičkom napadu odmah započete aktivnosti izvješćivanja Sigurnosno-obavještajne agencije (SOA-e), Centra za kibernetičku sigurnost (CKS) i Ministarstvo unutranjih poslova (MUP), kao i AZOP te je od svih zatraženo savjetovanje o ključnim aspektima odgovora na incident i oporavak od njega, da uzimajući u obzir da bi informiranje i iznošenje podataka tijekom istrage protivno postupanju navedenih nadležnih tijela, a postupanje s osjetljivim podacima o nacionalnoj kritičnoj infrastrukturi podliježe posebnim propisima iz područja informacijske sigurnosti te bi posljedično moglo ugroziti legitimne interese u provedbi istrage o okolnostima sigurnosnog incidenta, navodi se da Bolnica X nije izravno kontaktirao i pojedinačno obavještavao ispitanike u smislu članka 34. Opće uredbe o zaštiti podataka.
Dalje se navodi da s obzirom na veliki opseg korisnika Bolnice X, da se od početka sigurnosnog incidenta održava stalna komunikacija s javnošću putem konferencija za medije, sudjelovanje u javnim medijima i emisijama javnog sadržaja i dr. te da su osim navedenog i nadležna tijela koja sudjeluju u postupku odgovora i oporavka od kibernetičkog napada pružala informacije i izvještavale javnost o incidentu.

Nastavno na zaprimljenu informaciju u svezi predmetne povrede kod voditelja obrade Bolnice X u kojoj se navodi da su nekim ispitanicima nedostupni određeni medicinski nalazi učinjenih pretraga iz prethodnih mjeseci te da nekih pacijenata nema u evidencijama bolničkog sustava kao da se nisu niti liječili, a da je voditelj obrade izjavio da podaci nisu nestali nego su u procesu vraćanja i

učitavanja nakon hakerskog napada, Agencija je dopisom KLASA:, URBROJ: zatražila od Bolnice X dodatno očitovanje i dokumentaciju da li su zaprimili usmene i pismene prigovore pacijenata/ispitanika u svezi nedostupnosti njihovih medicinskih nalaza/dokumentacija o liječenju, navesti njihov broj, kakav odgovor im je dan, te potkrijepiti isto relevantnim dokazima, zatim, u odnosu na izjavljeno u zapisniku o provedenom nadzoru u prostorijama Bolnice X *„da se podaci o pacijentima nalaze u Bolničkom informacijskom sustavu (BIS) koji se nalazi na CDU-u, i koji nije bio zahvaćen predmetnom povredom jer je pristup istom na vrijeme onemogućen*“, je zatraženo očitovanje na temelju kojih informacija je dana navedena izjava u zapisniku a koja je kontradiktorna s posljednjim informacijama voditelja obrade da su podaci u procesu vraćanja i učitavanja nakon hakerskog napada, da isto pokrijepe s relevantnim dokazima.

U odnosu na posljednje izjavljeno od strane voditelja obrade da podaci nisu nestali nego su procesu vraćanja i učitavanja nakon hakerskog napada zatraženo je očitovanje gdje se fizički nalaze pohranjeni podaci do kojih se trenutačno ne može doći, o kojoj količini podataka je riječ, te kolikom broju pacijenata/ispitanika trenutačno nisu dostupni u procesu redovnog liječenja.

Agencija je zaprimila očitovanje od voditelja obrade Bolnice X kojim se navodi da su odmah nakon kibernetičkog napada prema prioritetima provjereni svi informatički sustavi Bolnice X važni za kontinuirano pružanje zdravstvene skrbi pacijenata, da su Bolnički informacijski sustav (BIS), Radiološki informacijski sustav (RIS) i sustav za pohranu slikovnog materijala (PACS) provjeravani s najvišim prioritetom, medicinska dokumentacija (nalazi) pohranjeni u BIS-u i RIS-u nije bila zahvaćena kibernetičkim napadom te je dostupna cijelo vrijeme za sve pacijente, da također, ništa od slikovnog materijala i videozapisa (radiološki, patološki) nije izgubljeno, otuđeno ili oštećeno, i svaki pacijent koji zatraži može dobiti svoje slikovne materijale u digitalnom obliku, da je zbog preventivnog razloga pokrenut proces migracije slikovnog materijala na Centar dijeljenih usluga (CDU) te je potrebno skenirati i provjeravati slikovni materijal generiran unutar dvije godine, što podrazumijeva više od 400 milijuna datoteka (cca 60 TB podataka). Isto se navodi da se pisani zahtjevi za slikovnim materijalom pacijenata i vodećih liječnika obrađuju unutar 30 minuta nakon čega je slikovni materijal dostupan a da x zavod nije zaprimio ni usmene ni pisane prigovore pacijenata u vezi nedostupnosti medicinske dokumentacije.

Agencija je zaprimila dodatno očitovanje od voditelja obrade Bolnice X nastavno na prethodno dostavljene informacije, kojim se navodi da u svezi medijski prenesene informacije i intervju pacijentice XY o nedostupnosti njezinog slikovnog materijala, slikovni materijal nije izgubljen, otuđen ili oštećen te da svaki pacijent koji zatraži može dobiti svoje slikovne materijale u digitalnom obliku, da iz sada podnesenih izvješća o statusu informacijskih sustava u Bolnici X proizlazi da je PACS sustav u kojem je pohranjen slikovni materijal oporavljen. Očitovanju se prilažu radiološki nalazi i slikovni materijal (na CD-u) imenovane pacijentice.

Agencija se dopisom KLASA:, URBROJ: obratila voditelju obrade Bolnici X i zatražila očitovanje koliki se ukupan broj zaposlenika Bolnice X s njihovim osobnim podacima nalazio na sustavima pohrane koji su bili zahvaćeni predmetnom povredom, koliki je ukupan broj pacijenata s njihovim osobnim podacima nalazio na sustavima pohrane koji su bili zahvaćeni

predmetnom povredom, koliki je ukupan broj medicinskih nalaza odnosnih na pacijente i dijagnostičkih slikovnih materijala nalazio na sustavima pohrane koji su bili zahvaćeni predmetnom povredom i bili nedostupni do oporavka sustava, te navesti koje vrste dijagnostičkih pretraga su bile odgođene ili otežane zbog predmetne povrede.

Agencija je zaprimila očitovanje od voditelja obrade Bolnice X nastavno na dopis Agencije kojim isti između ostalog navodi da je dostavio očitovanje kojim nastavno na prethodna izvješća navodi da je nakon kibernetičkog napada izvršena provjera svih informatičkih sustava važnih za kontinuirano pružanje zdravstvene skrbi pacijentima te da su Bolnički informacijski sustav (BIS), Radiološki informacijski sustav (RIS) i sustav za pohranu slikovnog materijala (PACS) provjeravani s najvišim prioritetom, da je također navedeno da je BIS na kojem se pohranjuju osobni podaci pacijenata smješten u Centru dijeljenih usluga (CDU) kao dio državne informacijske infrastrukture budući Bolnica X predstavlja nacionalnu kritičnu infrastrukturu i s tim u svezi napominje da su sustavi RIS (Radiološki nalazi) i LIS (Laboratorijski informacijski sustav) sastavni dio bolničkog informacijskog sustava Bolnice X, da vezano uz upit o broju zaposlenika Bolnice X i njihovim osobnim podacima koji su se nalazili na sustavima pohrane koji su bili zahvaćeni predmetnom povredom, dodatno pojašnjava da je HR sustav (Ljudski resursi) također sastavni dio integriranog bolničkog informacijskog sustava koji se nalazi na CDU.

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.

Sukladno članku 4. stavku 1. točki 1. Opće uredbe o zaštiti podataka, osobni podaci su 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.

Sukladno članku 4. stavku 1. točki 2. Opće uredbe o zaštiti podatka, obrada znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.

Člankom 5. stavkom 1. Opće uredbe o zaštiti podataka propisano je da osobni podaci moraju biti zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika (načelo zakonitosti, poštenosti i transparentnosti); 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); primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju (načelo smanjenja količine podataka); točni i prema potrebi ažurni (načelo točnosti); čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi

kojih se osobni podaci obrađuju (načelo ograničenja pohrane) i obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neodgovarajuće ili nezakonite obrade te od slučajnog gubitka ili uništenja, primjenom odgovarajućih tehničkih ili organizacijskih mjera (načelo cjelovitosti i povjerljivosti).

Člankom 25. stavkom 1. Opće uredbe o zaštiti podataka propisano je da uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava ispitanika.

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

Provedenim uvidom u cjelokupnu dokumentaciju spisa predmeta, u ovoj upravnoj stvari utvrđeno je da je voditelj obrade Bolnica X, zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera sigurnosti obrade osobnih podataka sukladno predvidivim rizicima omogućio nepoznatoj osobi/napadaču da ostvari pristup osobnim podacima u informacijskom sustavu istog voditelja obrade te kopirao / iznosio podatke u količini od najmanje 3 GB izvan sustava voditelja obrade.

Utvrđeno je da je napadač najvjerojatnije socijalnim inženjeringom došao u posjed pristupnih podataka (korisničko ime i lozinka) zaposlenika Bolnice X te putem VPN konekcije ostvario prvo spajanje na informacijski sustav voditelja obrade, nakon čega je iskoristio slabost istog sustava i osigurao prava domenskog korisničkog računa koji je imao najviše privilegije na sustavu (Domain admin), a koji se upotrebljava kao servisni račun za potrebe rada sustava koji isporučuje vanjsko društvo. Dalje je utvrđeno da je napadač na domenski kontroler prenio datoteku kojom je proveo skeniranje cijele unutarnje komunikacijske mreže i koji je proces mrežnog skeniranja završio.

Utvrđeno je da je prvo Remote Deskotop Protocol (RDP) spajanje napadača s korisničkim računom zabilježeno te da je isti dalje instalirao na domenske kontrolere administrativne alate za udaljeni pristup.

Utvrđeno je da je napadač proveo uspješno RDP spajanje s računom na poslužitelj kojom prilikom je obrisao sigurnosne kopije (eng. backup), a da je istog dana započeo proces kriptiranja poslužitelja i domenskih kontrolera.

Utvrđeno je da je napadač svoje napade/uspješan ulazak i daljnje ulaske u informacijski sustav voditelja obrade, provodio s IP adrese koja geolokacijski pripada Rumunjskoj.

Utvrđeno je dostavljenim očitovanjem voditelja obrade koji su serveri zahvaćeni predmetnom povredom i kriptirani od strane napadača.

Utvrđeno je da kompromitirani FileShare, u koji je izvršen uvid tijekom nadzora ima instaliran operativni sustav Windows 2008 R2 Standard za koji je prestala podrška proizvođača, te da se na istom File Share-u nalaze podaci odnosni na ispitanike, točnije medicinski podaci, a koji se smatraju posebna kategorija osobnih podataka i da izravan pristup njima nije bio ograničen dodatnom tehničkom mjerom zaštite kao npr. lozinkom ili da su podaci bili pseudonimizirani.

Utvrđeno je da je napadač na dijelove informacijskog sustava Bolnice X kojima je ostvario pristup instalirao servise, a koje je koristio za sve neovlaštene radnje unutar istog sustava.

U ovoj upravnoj stvari utvrđeno je da je Bolnica X kao voditelj obrade učinio višestruke propuste kod implementacije odgovarajućih mjera sigurnosti obrade osobnih podataka. S tim u svezi, udaljeni pristup informacijskom sustavu Bolnice X putem VPN konekcije, unatoč postojanju javno dostupne informacije o kibernetičkoj ugrozi VPN konekcija na globalnoj razini više od godinu dana i trendova kibernetičkih kriminalnih skupina da iskorištavaju slabosti VPN konekcije uz primjenu različitih tehnika proboja u informacijske sustave voditelja obrade diljem svijeta, nije bio pravovremeno osnažen putem implementacije dodatne 2-faktorske autentifikacije (dalje u tekstu: 2-FA), a koja bi dodatnim korakom provjere identiteta korisnika možebitno spriječila napadača u ulasku u informacijski sustav Bolnice X, odnosno osigurala viši nivo zaštite od neovlaštenog pristupa.
Posebnu težinu ovom propustu daje činjenica da je u trenutku predmetne povrede bilo aktivnih xy korisnika (zaposlenika) i xy vanjskih dobavljača/suradnika koji imaju ovlasti spajanja putem VPN-a na informacijski sustav Bolnice X što predstavlja rizik kojem je bilo potrebno posvetiti dužnu pažnju kod dizajniranja mjera informacijske sigurnosti.

Dodatno, utvrđeno je da je voditelj obrade, u vrijeme određivanja sredstava obrade i u vrijeme same obrade, nemarom propustio posvetiti pažnju, konfiguriranju sigurnosnih mjera udaljenog pristupa i ograničiti pristup svom informacijskom sustavu samo s IP adresa koje geolokacijski pripadaju Republici Hrvatskoj. Taj aspekt sigurnosti ostao je zanemaren te je napadač svoj napad/uspješan ulazak i daljnje ulaske u sustav voditelja obrade, provodio s IP adrese koja geolokacijski pripada Rumunjskoj, koja funkcionalnost predstavlja propust voditelja obrade s

obzirom na činjenicu da svi zaposlenici, među kojima je i kompromitirani korisnički račun, imaju prebivalište u Republici Hrvatskoj, a tvrtke suradnici poslovni nastan u Republici Hrvatskoj, te je slijedom navedenog voditelj obrade trebao ograničiti pristup svojem sustavu samo na IP adrese koje geolokacijski pripadaju Republici Hrvatskoj.

Utvrđenje da je napadač kada je ostvario pristup informacijskom sustavu Bolnice X obrisao sigurnosnu kopiju (back-up) ukazuje da je ista bila smještena na neodgovarajućoj domeni i lako dostupna čime je ugrožena obrada, odnosno osobni podaci sadržani u sustavima pohrane, te je voditelj obrade propustio izdvojiti backup poslužitelj iz domene, odnosno, organizacijskom i tehničkom mjerom osigurati da se backup nalazi van domene, te dodatno da osigura postojanje redovno ažurirane backup kopije izvan informacijskog sustava Bolnice X na dislociranoj fizičkoj lokaciji, npr. drugi podatkovni centar.

Voditelj obrade Bolnice X je u svojim očitovanjima u nekoliko navrata naveo da ima implementiran PAM sustav za nadzor privilegiranih korisničkih računa, te rješenje za detekciju malicioznog ponašanja na mreži (NDR), ali kako je iz provedenog postupka utvrđena kompromitacija administratorskog računa kojim je napadač neometano provodio aktivnosti unutar informacijskog sustava voditelja obrade koje ne odgovaraju uobičajenim aktivnostima istog administratorskog računa i izvan uobičajenog radnog vremena voditelja obrade i zaposlenika, proizlazi da navedeni PAM sustav pa i NDR nisu bili konfigurirani s dužnom pažnjom da aktivnosti napadača budu pravovremeno uočene, istražene i obaviještene odgovorne osobe, odnosno, adekvatno detektirane/prepoznate anomalije/ neuobičajene aktivnosti, te posljedično cjelovitost i integritet sustava s velikom vjerojatnošću ne bi bili kompromitirani/ probijeni, a osobni podaci ne bi bili učinjeni dostupni napadaču.

Uzimajući u obzir činjenicu da je Bolnica X temeljem Zakona o kritičnim infrastrukturama (NN 114/22) određena nacionalnom kritičnom infrastrukturom u sektoru zdravstva, da obrađuje veliki opseg posebne kategorije osobnih podataka, da je u trenutku predmetne povrede imao xy internih (zaposlenici) i xy vanjskih (dobavljači/suradnici) VPN korisnika, da je napadač u informacijskom sustavu Bolnice X boravio gotovo 7 dana neprimijećeno, ulazio u sustav izvan redovnog radnog vremena, da je pokretao izvršne datoteke (.exe) za potrebe neovlaštenih aktivnosti, iznosio podatke izvan istog sustava, proizlazi da je voditelj obrade propustio prepoznati postojeće i predvidive rizike i implementirati odgovarajuće tehničko rješenje koje će u realnom vremenu pratiti aktivnosti unutar sustava te pravovremeno putem predefiniranih mjera (alarma/automatskih akcija) onemogućiti neovlaštene aktivnosti unutar sustava i/ili obavijestiti odgovorne osobe za nadzor informacijskog sustava o istome. Takvo rješenje, Security Information and Event Management (SIEM) postoji dovoljno dugo na tržištu da je voditelj obrade mogao pravovremeno implementirati i dizajnirati isti za centralno prikupljanje i analizu logova te za izvještavanje sigurnosno operativnog centra za pravovremenu i odgovarajuću reakciju na incident /povredu u realnom vremenu.

Također, iako voditelj obrade zapošljava oko xy ljudi, zanemario je veličinu i kompleksnost svog informacijskog sustava i nije poduzeo pravovremene, i dovoljne, odnosno, odgovarajuće organizacijske i tehničke mjere sigurnosti prije sigurnosnog incidenta/predmetne povrede

osobnih podataka, a koje su mogle, odnosne trebale svesti rizik iste ili slične povrede na najmanju moguću razinu.

Slijedom svega navedenog, utvrđeno je da je voditelj obrade učinio višestruke propuste prilikom dizajniranja sustava obrade, uključivo, ograničavanje pristupa, nadzor, izvješćivanje, pravovremeno reagiranje i uključivanje odgovarajućih korektivnih akcija u sustavu.

Iz prethodno navedenih odredbi Opće uredbe o zaštiti podataka proizlazi da je voditelj obrade prilikom obrade osobnih podataka dužan poduzeti odgovarajuće organizacijske i tehničke mjere sigurnosti, na način da treba osigurati trajnu povjerljivost sustava kao i proces redovnog testiranja, ocjenjivanja i procjenjivanja učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, a prilikom procjene odgovarajuće razine sigurnosti u obzir posebno uzeti rizike od, *inter alia*, neovlaštenog otkrivanja osobnih podataka. Nakon točno i potpuno utvrđenog činjeničnog stanja razvidno je da je voditelj obrade propustio provesti odgovarajuće tehničke i organizacijske mjere sigurnosti sukladno postojećim i predvidivim rizicima, čime je postupio protivno odredbama članka 32. stavka 1. točke b) i d) i stavka 2. Opće uredbe o zaštiti podataka.

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.

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 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 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 izvršitelja/voditelja obrade koji obrađuju osobne podatke ispitanika u području informacijskih tehnologija. Izricanjem upravne novčane kazne treba se postići generalno odvraćanje (obeshrabriti druge u ponavljanju kršenja u budućnosti), kao i posebno odvraćanje (obeshrabriti adresata ove upravne novčane kazne od ponavljanja kršenja).

Sukladno Smjernicama Radne skupine iz članka 29. o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 od 3. listopada 2017. godine (WP 253), a koje je Europski odbor za zaštitu podataka podržao na svojoj prvoj plenarnoj sjednici 25. svibnja 2018. godine, kako bi se osigurala postojana i visoka razina zaštite pojedinaca te uklonile prepreke protoku osobnih podataka unutar Unije, razina zaštite trebala bi biti jednaka u svim državama članicama (uvodna izjava 10 Opće uredbe o zaštiti podataka). U uvodnoj izjavi 11 pojašnjava se činjenica da su za jednaku razinu zaštite osobnih podataka diljem Unije potrebne, među ostalim, "jednake ovlasti praćenja i osiguravanja poštovanja pravila za zaštitu osobnih podataka i jednake sankcije za kršenja u državama članicama". Nadalje, kako je navedeno u uvodnoj izjavi 13, jednake sankcije u svim državama članicama te učinkovita suradnja među nadzornim tijelima različitih država članica potrebni su da bi se "spriječila razilaženja koja ometaju slobodno kretanje osobnih podataka na unutarnjem tržištu".

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.;
(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 4. točki (a) Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade u skladu s člankom 32. 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.

Uvodnom izjavom 150 Opće uredbe o zaštiti podataka navodi 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.

Sukladno Smjernicama Radne skupine iz članka 29. o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 od 3. listopada 2017. godine (WP 253), a koje je Europski odbor za zaštitu podataka podržao na svojoj prvoj plenarnoj sjednici 25. svibnja 2018. godine, kako bi nadzorno tijelo izreklo novčanu kaznu koja je učinkovita, proporcionalna i odvraćajuća, ono primjenjuje definiciju pojma poduzetnika kako ju je naveo Sud Europske unije za potrebe primjene članaka 101. i 102. UFEU-a, to jest smatra se da koncept poduzetnika znači gospodarsku jedinicu koju mogu osnovati matično društvo i sva uključena društva kćeri. U skladu s pravom EU-a i sudskom praksom, pojam poduzetnika treba shvatiti kao gospodarsku jedinicu koja se bavi komercijalnim/gospodarskim djelatnostima bez obzira na uključenu pravnu osobu.

U navedenim Smjernicama navode se i definicije pojma "poduzetnik" iz odluka Suda Europske Unije: Pojam "poduzetnik" obuhvaća svaki subjekt "koji obavlja gospodarsku djelatnost, neovisno o pravnom statusu tog subjekta i načinu njegova financiranja". Pojam poduzetnika

“mora se smatrati izrazom kojim se označava gospodarska jedinica čak i ako se u pravu ta gospodarska jedinica sastoji od nekoliko osoba, bilo fizičkih ili pravnih.“.

Uvidom u dostupne informacije Agencija je utvrdila da je Bolnica X (MBS:, OIB:) samostalni pravni subjekt.

Budući da ukupni godišnji prihodi u 2023. godini za Bolnicu X iznosi 566.232.915,37 EUR, 2% tog iznosa je 11.324.658,30 EUR, isti predstavlja gornju granicu za izricanje upravne novčane kazne u konkretnom slučaju, jer je navedeni iznos veći od 10.000.000,00 EUR.

Agencija je radi kršenja članka 32. stavka 1. točke b) i d) te stavka 2. Opće uredbe o zaštiti osobnih podataka izrekla voditelju obrade Bolnici X upravnu novčanu kaznu u iznosu od 20.000,00 EUR, a koji iznos čini 0,17% u odnosu na maksimalni iznos upravne novčane kazne koju je u konkretnom slučaju Agencija mogla, odnosno bila ovlaštena izreći.

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 1. izreke ovog rješenja, došlo je do kršenja obveza voditelja obrade iz članka 32. stavka 1. točke b) i d) te stavka 2. Opće uredbe o zaštiti podataka, neprovođenjem odgovarajućih tehničkih i organizacijskih mjera sigurnosti obrade osobnih podataka od strane voditelja obrade Bolnice X a za koje kršenje Opća uredba o zaštiti podataka propisuje izricanje upravne novčane kazne sukladno članku 83. stavku 4. točke a), odnosno, 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 što je veće.

Sukladno Smjernicama o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679, pokazatelj težine kršenja može biti ne samo priroda kršenja, već i opseg, svrha predmetne obrade kao i broj ispitanika i razina štete koju su pretrpjeli.

U predmetnoj povredi nije bilo moguće utvrditi točan broj ispitanika čiji su osobni podaci, zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera zaštite informacijskog sustava voditelja obrade, učinjeni dostupnima neovlaštenoj osobi/napadaču, kao niti količina izvezenih podataka izvan sustava, ali je utvrđeno da se radi o broju ne manjem od onih ispitanika sadržanih na kompromitiranom File Share-u koji je pregledan tijekom provedbe nadzornog postupanja. Nadalje, iako predmetna povreda može biti sagledana u vremenskom okviru od prvog uspješnog ulaska napadača u informacijski sustav voditelja obrade do dana kada je voditelj obrade postao svjestan povrede i poduzeo mjere za rješavanje iste, kršenje odredbi Opće uredbe o zaštiti podataka voditelja obrade zapravo traje od 25. svibnja 2018. od pune

primjene Opće uredbe o zaštiti podataka jer voditelj obrade nije implementirao odgovarajuće mjere sigurnosti koje su mogle, odnosne trebale svesti rizik iste ili slične povrede na najmanju moguću razinu.

Tijekom postupka nije utvrđeno da li su ispitanici pretrpjeli određenu štetu kao posljedicu predmetne povrede.

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

Radna skupina iz članka 29 navodi u Smjernicama o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 da "namjera" u pravilu uključuje znanje i nakanu u pogledu značajki prekršaja, dok "nenamjerno" znači da nije postojala namjera da se prouzroči kršenje iako je voditelj obrade/izvršitelj obrade prekršio svoju obvezu dužne pažnje propisanu zakonom. Iste Smjernice dakle naglašavaju razliku između okolnosti koje su indikativne ili „namjerne povrede" i onih koje ukazuju na kršenja koja su prouzročena „nenamjerno" ili "nemarom". U tom smislu Smjernice navode "ne donošenje politika" i "ljudsku pogrešku" kao primjere ponašanja koji mogu ukazivati na nepažnju.

U odnosu na navedeno, u predmetnom slučaju nije utvrđeno da je bilo izravne namjere kršenja odredbi Opće uredbe o zaštiti podataka od strane Bolnice X, ali je utvrđen nemar i nedostatak radnji koje bi prevenirale povredu. Naime, u ovoj upravnoj stvari utvrđeno je da je Bolnica X kao voditelj obrade propustio primijeniti odgovarajuće organizacijske i tehničke mjere zaštite kako bi zaštitio osobne podatke koje obrađuje, odnosno zaštitio osobne podatke od uništenja, izmjene, zabranjenog odavanja i neovlaštenog pristupa, što je za posljedicu imalo da je napadač jednom kada je ostvario pristup na sustav voditelja obrade neometano i neopaženo ostvario pristup osobnim podacima ispitanika na više poslužitelja a čime su ispunjeni svi elementi grube nepažnje u postupanju.

- 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 saznanje o predmetnoj povredi Bolnica X je odmah pristupila rješavanju nastalog sigurnosnog problema na način da je neposredno po kibernetičkom napadu odmah započela aktivnosti izvješćivanja Sigurnosno-obavještajne agencije (SOA-e), Zavoda za sigurnost informacijskih sustava (ZSIS) i Ministarstva unutarnjih poslova (MUP), te je angažirao specijalističku tvrtku iz područja informatike da provede forenzičku analizu sustava i mjere za povrat sustava u operativno stanje.

- 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);

Uzimajući u obzir odredbe članka 32. koje obvezuju voditelja obrade i izvršitelja obrade da provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu

sigurnosti s obzirom na rizik, uključujući prema potrebi: sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade; proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, da se prilikom procjene odgovarajućeg nivoa sigurnosti 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, utvrđeno je da Bolnica X provodi određene organizacijske i tehničke mjere zaštite pri obradi osobnih podataka, ali da u konkretnom slučaju nisu bile dovoljne čime je došlo do neovlaštenog pristupa i iznošenje osobnih podataka ispitanika.
Naime, u ovoj upravnoj stvari utvrđeno je da je Bolnica X kao voditelj obrade učinio višestruke propuste prilikom dizajniranja sustava obrade, uključivo, ograničavanje pristupa, nadzor, izvješćivanje, pravovremeno reagiranje i uključivanje odgovarajućih korektivnih akcija u sustavu.

Voditelj obrade je nemarom propustio posvetiti pažnju u trenutku dizajniranja sustava i kasnije tijekom same obrade, konfiguriranju sigurnosnih mjera udaljenog pristupa i ograničiti pristup svom informacijskom sustavu samo s IP adresa koje geolokacijski pripadaju Republici Hrvatskoj. Taj aspekt sigurnosti ostao je zanemaren te je napadač svoj napad/uspješan ulazak i daljnje ulaske u sustav voditelja obrade, provodio s IP adrese koja geolokacijski pripada Rumunjskoj, koja funkcionalnost predstavlja propust voditelja obrade s obzirom na činjenicu da svi zaposlenici, među kojima je i kompromitirani korisnički račun imaju prebivalište u Republici Hrvatskoj, a tvrtke suradnici poslovni nastan u Republici Hrvatskoj, te je slijedom navedenog voditelj obrade trebao ograničiti pristup svojem sustavu samo na IP adrese koje geolokacijski pripadaju Republici Hrvatskoj.
Voditelj obrade je unatoč postojanju javno dostupne informacije o kibernetičkoj ugrozi VPN konekcija na globalnoj razini više od godinu dana i trendova kibernetičkih kriminalnih skupina da iskorištavaju slabosti VPN konekcije uz primjenu različitih tehnika proboj u informacijske sustave voditelja obrade diljem svijeta, propustio implementirati dodatnu 2-faktorske autentifikacije (2-FA), a koja bi dodatnim korakom provjere identiteta korisnika s velikom vjerojatnošću spriječila napadača u ulasku u informacijski sustav Bolnice X odnosno osigurala viši nivo zaštite od neovlaštenog pristupa, uzimajući u obzir da je u trenutku predmetne povrede bilo aktivnih xy korisnika (zaposlenika) i xy vanjskih dobavljača/suradnika koji imaju ovlasti spajanja putem VPN-a na informacijski sustav Bolnice X.

Činjenica da je napadač kada je ostvario pristup informacijskom sustavu Bolnice X obrisao sigurnosnu kopiju (back-up) ukazuje da je ista bila smještena na neodgovarajućoj domeni i lako dostupna čime je ugrožena obrada, odnosno osobni podaci sadržani u sustavima pohrane, te je voditelj obrade propustio izdvojiti back-up poslužitelj iz domene, odnosno, organizacijskom i tehničkom mjerom osigurati da se backup nalazi van domene, te dodatno da osigura postojanje redovno ažurirane back-up kopije izvan informacijskog sustava Bolnice X na dislociranoj fizičkoj lokaciji, npr. drugi podatkovni centar.

PAM sustav za nadzor privilegiranih korisničkih računa i NDR rješenje za detekciju malicioznog ponašanja na mreži koje Bolnica X navodi da su implementirani u njihovom informacijskom sustavu, nisu bili s dužnom pažnjom konfigurirani imajući u vidu da je napadač koristio kompromitirani administratorski račun s kojim je neometano provodio aktivnosti unutar informacijskog sustava voditelja obrade, koje ne odgovaraju uobičajenim aktivnostima istog administratorskog računa i izvan uobičajenog radnog vremena voditelja obrade i zaposlenika, pri čemu njegove aktivnosti nisu pravovremeno uočene, istražene i obaviještene odgovorne osobe, odnosno, adekvatno detektirane/prepoznate anomalije/neuobičajene aktivnosti, te je posljedično cjelovitost /integritet sustava bila narušena i došlo je do predmetne povrede.

S obzirom na kompleksnost informacijskog sustava, velikog broja zaposlenika koji istom pristupaju lokalno i udaljeno, velikom broju osobnih podataka osnovne i posebne kategorije koje obrađuje, voditelj obrade je propustio implementirati odgovarajuće tehničko rješenje, kao što je npr. SIEM koje će u realnom vremenu pratiti aktivnosti unutar sustava te pravovremeno putem predefiniranih mjera (alarma/automatskih akcija) onemogućiti neovlaštene aktivnosti unutar sustava i/ili obavijestiti odgovorne osobe za nadzor informacijskog sustava o istome, a imajući u vidu da je napadač u informacijskom sustavu Bolnice X boravio gotovo 7 dana neprimijećeno, ulazio u sustav izvan redovnog radnog vremena, da je pokretao izvršne datoteke (.exe) za potrebe neovlaštenih aktivnosti i iznosio podatke izvan istog sustava, a što je navedenim tehničkim rješenjem moglo biti pravovremeno uočeno.

Voditelj obrade je zanemario i činjenicu da je na kompromitiranom File Share-u u trenutku predmetne povrede bio instaliran operativni sustav Windows 2008 R2 Standard za koji je prestala podrška proizvođača 14.01.2020., čime je ranjivost istog višestruko uvećana, da se na istom File Share-u nalaze podaci odnosni na ispitanike, točnije medicinski podaci/nalazi, odnosno osobni podaci o zdravlju, a koji se smatraju posebnom kategorijom osobnih podataka, te da izravan pristup njima nije bio ograničen dodatnom tehničkom mjerom zaštite kao npr. lozinkom ili da su podaci bili pseudonimizirani.

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

Prema evidencijama kršenja koje vodi ova Agencija, voditelj obrade Bolnica X nije u prošlosti počinio istovjetno kršenje niti je prekršio Opću uredbu o zaštiti podataka na istovjetan način.

- 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 Bolnica X je tijekom ovog upravnog postupka pravovremeno odgovarala na zahtjeve nadzornog tijela. Međutim, iz informacija dobivenih u očitovanjima i utvrđenjima u provedenom nadzoru na adresi poslovnog nastana istog, proizlaze kontradiktornosti činjeničnog stanje u pogledu koji su sve poslužitelji bili kompromitirani odnosno kriptirani od

strane napadača, koliko je osobnih podataka zaposlenika i pacijenata zahvaćenih predmetnom povredom te konačno koliko je medicinskih nalaza bilo nedostupno pacijentima.
Naime, prvim očitovanjem Bolnica X je navela da je „*kriptiran dio sadržaja na backup serveru, te sadržaj radiološkog informacijskog sustava",* da bi kasnijem očitovanjem naveo "*da su Bolnički informacijski sustav (BIS), Radiološki informacijski sustav (RIS) i sustav za pohranu slikovnog materijala (PACS) provjeravani s najvišim prioritetom, medicinska dokumentacija (nalazi) pohranjeni u BIS-u i RIS-u nije bila zahvaćena kibernetičkim napadom te je dostupna cijelo vrijeme za sve pacijente",* a Izvješće o provedenoj analizi incidenta, na str. 7 navodi „*S obzirom kako se došlo do saznanja kako je napadač izbrisao sigurnosne kopije (engl. Backup), ovo potvrđuje napadačevu prisutnost na navedenom poslužitelju i implicira daljnje aktivnosti brisanja sigurnosnih kopija. Navedena taktika napadača je uobičajena, a koja je svrha onemogućiti žrtvu u aktivnostima oporavka i prisiliti ju dodatno na plaćanje iznude.*"

Dopisom Bolnica X navodi servere koji su zahvaćeni predmetnom povredom i kriptirani od strane napadača, njih 24, da bi tijekom nadzora predstavnik voditelja obrade izjavio da je kompromitiran samo File Share (također prethodno naveden u dopisu).

Nadalje, nastavno na informacije iznesene u medijima o nedostupnosti određenih medicinskih nalaza učinjenih pretraga iz prethodnih mjeseci, uz navođenje konkretnog imena i prezimena pacijentice kojoj je liječnik rekao da mu njezini nalazi nisu dostupni da joj ih da na uvid, i da je voditelj izjavio da podaci nisu nestali nego se u procesu vraćanja i učitavanja hakerskog napada, Agencija je dopisom zatražila od voditelja obrade da pojasni isto s obzirom na prethodno izjavljeno u zapisniku o provedenom nadzoru*"da se podaci o pacijentima nalaze u Bolničkom Informacijskom Sustavu (BIS) koji se nalazi na CDU-u i koji nije bio zahvaćen predmetnom povredom, da se svi podaci vezani za zaposlenike nalaze na CDU-u i također nisu bili zahvaćeni predmetnom povredom jer je pristup istima na vrijeme onemogućen".* Voditelj obrade u svezi prethodnog je očitovanjem izjavio „*da Medicinska dokumentacija pacijenata (nalazi) pohranjena u Bolničkom informacijskom sustavu (BIS) i Radiološkom informacijskom sustavu (RIS), nije bila zahvaćena kibernetičkim napadom te je dostupna cijelo vrijeme za sve pacijente*," što je kontradiktorno spram informacija iznesenih u medijima od pacijenta, liječnika pa i službene izjave voditelja obrade dane istom mediju, jer ako nalazi pacijenata nisu bili zahvaćeni predmetnom povredom zašto su onda „nedostupni" liječniku i pacijentu 4 mjeseca nakon predmetne povrede, te ako su "u procesu vraćanja i učitavanja nakon hakerskog napada," ne mogu istovremeno biti u statusu "da nisu bili zahvaćeni istim napadom te dostupni cijelo vrijeme za sve pacijente".

Prema zaprimljenom dopisu u Agenciji Bolnica X dodatno navodi „*da iz sada podnesenih izvješća o statusu informacijskih sustava u Bolnici X proizlazi da je PACS sustav u kojem je pohranjen slikovni materijal oporavljen",* što je kontradiktorno informaciji danoj u zapisniku kada se spominje samo File Share koji je bio kompromitiran predmetnom povredom i informaciji iz očitovanja kojem se navode 24 servera/poslužitelja koji su kriptirani (kompromitirani) među kojima je i PACS.

Dodatno u svezi prethodnog valja spomenuti da je voditelj obrade tijekom nadzora pojasnio da „*broj ispitanika od xy naveden u dopuni Izvješća o povredi osobnih podataka je odnosan na*

ukupan broj ispitanika kojima kompromitirani dijelovi informacijskog sustava nisu bili dostupni te ne predstavlja broj ispitanika čiji su osobnih podaci kompromitirani,“, čime se može u konačnici izvesti zaključak da voditelj obrade nije na adekvatan način pristupio utvrđenju broja ispitanika zahvaćenih predmetnom povredom kao niti sve okolnosti vezane uz istu.

Također iako je tijekom nadzora izvršenim nasumičnim uvidom u nekoliko mapa na kompromitiranom File Share-u utvrđeno postojanje određenog broja dokumentacije koja sadrži osobne podatke (identifikacije, slike i dr.) i podatke o zdravlju, odnosno posebne kategorije osobnih podataka ispitanika, voditelj obrade tijekom daljnjeg postupka na zahtjev da dostavi podatak koliki se ukupan broj pacijenata s njihovim osobnim podacima nalazio na sustavima pohrane koji su bili zahvaćeni predmetnom povredom, koliki je ukupan broj medicinskih nalaza odnosnih na pacijente i dijagnostičkih slikovnih materijala nalazio na sustavima pohrane koji su bili zahvaćeni predmetnom povredom i bili nedostupni do oporavka sustava, te navesti koje vrste dijagnostičkih pretraga su bile odgođene ili otežane zbog predmetne povrede, je paušalno odgovorio da „*ništa od slikovnog materijala i videozapisa (radiološki, patološki) nije izgubljeno, otuđeno ili oštećeno, i svaki pacijent koji zatraži može dobiti svoje slikovne materijale u digitalnom obliku“,* pri čemu nije izravno dao informacije/podatke vezane niti uz utvrđenja za File Share niti za cjelokupni informacijski sustav iako iz spisa predmeta proizlazi da se radi o značajnom broju ispitanika.

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

Tijekom postupka je utvrđeno da je nepoznatoj osobi bila dostupna osnovna kategorija osobnih podataka, ime, prezime, adresa, broj telefona, email, bankovni račun, ali i posebna kategorija osobnih podataka kao što su medicinski podaci sadržani u nalazima kliničkih istraživanja pohranjeni na kompromitiranom poslužitelju.

- 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);

Člankom 33. stavkom 1. Opće uredbe o zaštiti podataka propisano je da 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 33. 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.
Za predmetnu povredu nadzorno tijelo je saznalo putem medija, odnosno informacija objavljenih u medijima, te nakon što se pisanim putem obratilo voditelju obrade Bolnici X, zaprimilo je Izvješće o povredi osobnih podataka sukladno članku 33. Opće uredbe o zaštiti podataka.

- 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);

Voditelju obrade Bolnici X u vezi s istim predmetom nije prethodno izrečena mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka.

- 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);
Nije utvrđeno da je Bolnica X ostvarila financijsku dobit kršenjem niti izbjegnula gubitke, izravno ili neizravno.

Zaključno, iz svega navedenog proizlazi da je voditelj obrade Bolnica X propustila provesti odgovarajuće tehničke i organizacijske mjere sigurnosti obrade sukladno postojećim i predvidivim rizicima, a koje mjere su mogle spriječiti/umanjiti nastalu opisanu povredu osobnih podataka ispitanika, čime je postupila protivno odredbama članka 32., stavka 1. točke b) i d) i stavka 2. Opće uredbe o zaštiti podataka.

Jednako tako, uzimajući u obzir sve prethodno navedeno, Agencija smatra da je upravo korektivna mjera u vidu upravne novčane kazne učinkovita, proporcionalna i odvraćajuća 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 roku od 30 dana od dana dostave rješenja.

RAVNATELJ

Zdravko Vukić, univ. mag. oec.

DOSTAVITI:

1. Bolnica X
2. Pismohrana, ovdje