Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

BEZBEDNOST I ZAŠTITA PODATAKA O LIČNOSTI U ZDRAVSTVENIM USTANOVAMA

SECURITY AND PERSONAL DATA PROTECTION IN HEALTHCARE INSTITUTIONS

Pregledni naučni rad

Prof. dr Zoran Keković[462]
Prof. dr Gordana Pejović[463]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Stupanjem na snagu Opšte uredbe o zaštiti podataka (GDPR), kao i odgovarajućih nacionalnih propisa koji su transponovali odredbe ove uredbe u zakonodavstvo zemalja koje nisu članice EU, pred zdravstvene ustanove u regionu stavlja se nimalo lak zadatak da usklade svoje procedure sa ovim odredbama.

Ciljevi rada (naučni i/ili društveni): Cilj rada je da se omogući objedinjeni prikaz važećih bezbednosnih standarda, kao i odgovarajućih smernica za bezbednost u zdravstvu, čija primena omogućava veću bezbednost zaposlenih, pacijenata i drugih ljudi koji posećuju zdravstvene ustanove. Takođe, u radu će biti prikazani i regulatorni zahtevi koji se odnose na posebne kategorije podataka o ličnosti – podatke o zdravstvenom stanju.

Metodologija/Dizajn: U radu se daje pregled normativnih aspekata bezbednosti u zdravstvu, kao i zaštite podataka o ličnosti, faktičkom stanju u ovoj oblasti, te izazovima koje donose novi propisi u ovoj oblasti.

Ograničenja istraživanja/rada: Podaci o zdravstvenom stanju građana, kao posebno osetljivi podaci o ličnosti, podrazumevaju posebne mere zaštite i specifične tehničke, fizičke i organizacione kontrole, tako da je u radu prikazan samo jedan od mogućih pristupa u sprovođenju ovih mera.

Rezultati/Nalazi: Ističe se značaj adekvatnog razumevanja i primene odredaba zakonske regulative, kao i srazmernih kontrola za osiguranje bezbednosti lica i podataka o ličnosti.

Generalni zaključak: Naročite napore treba uložiti da se u zdravstvene ustanove implementiraju mere koje će garantovati bezbednost podataka o ličnosti, imajući u vidu istoriju čestih i ozbiljnih incidenata narušavanja ovih podataka.

Opravdanost istraživanja/rada: Opravdanost rada nalazi se u činjenici da je potrebno garantovati pacijentima, građanima i zaposlenima u zdravstvenim ustanovama adekvatan nivo zaštite podataka o ličnosti, ali i ličnu bezbednosti tokom procesa koje obavljaju.

[462] Univerzitet u Beogradu, Fakultet bezbednosti, zorankekovic@yahoo.com
[463] Univerzitet u Beogradu, Fakultet organizacionih nauka, SGS Beograd doo, gordana.pejovic@sgs.com

Ključne riječi
bezbednost, zaštita podataka o ličnosti, zdravstvena zaštita

Abstract
Reason for writing and research problem (s): By entering the General Data Protection Regulation (GDPR) into force, as well as the relevant national regulations transposing provisions of this Regulation into the legislation of non-EU countries, the healthcare institutions in the region got the complex task to harmonize their procedures with these provisions.
Aims of the paper: The aim of the paper is to provide a review of the applicable safety standards, as well as the relevant safety guidelines in healthcare, the application of which allows for greater safety of employees, patients and other people visiting health facilities. Also, the paper will show the regulatory requirements related to special categories of personal data – data concerning health.
Methodology: The paper presents a review of the normative aspects of safety in health care, as well as the protection of personal data, the factual situation in this field, and the challenges brought by the new regulations in this field.
Research/Paper Limitation: Data concerning health, as special category of personal data, imply special protection measures and special technical, physical and organizational controls, so that only one of the possible approaches in the implementation of these measures is presented in the paper.
Results / General Conclusion: The importance of adequate legal provisions understanding and implementation is emphasized, as well as the application of proportional controls for ensuring the safety of the person and personal data.
Conclusion: Efforts should be made to implement measures that will guarantee the protection of personal data in healthcare institutions, bearing in mind the history of frequent and serious breaches of healthcare data.
Research / Paper Validity: The justification of work is in the fact that it is necessary to guarantee patients, citizens and employees in healthcare institutions an adequate level of protection of personal data, as well as personal safety during the processes they perform.

Key words
safety, personal data protection, healthcare

Uvod

Zdravstvene ustanove, medicinski personal, kao i korisnici zdravstvenih usluga, uključujući i imovinu i osetljive informacije od značaja za te usluge, sve više su izloženi bezbednosnim rizicima ljudskog porekla.

Primena bezbednosnih standarda i odgovarajućih zakonskih propisa u zdravstvu može varirati u zavisnosti od tipa zdravstvene ustanove, zbog čega je važno da oni budu prilagođeni specifičnostima sredine i potrebama zaštite. *Direktivom EU o kritičnim infrastrukturama* (*2008/114/ES),* kao i *Zakonom o kritičnim infrastrukturama* (Službeni glasnik RS", broj 87 od 13. novembra 2018.) sektor zdravstva prepoznat je kao kritična infrastruktura

što pretpostavlja poseban nivo bezbednosti u cilju obezbeđivanja kontinuiteta zdravstvene zaštite u raznim uslovima. Takođe, stupanjem na snagu Opšte uredbe o zaštiti podataka (GDPR), kao i odgovarajućih nacionalnih propisa koji su transponovali odredbe ove uredbe u zakonodavstvo zemalja koje nisu članice EU, pred zdravstvene ustanove u regionu stavlja se nimalo lak zadatak da usklade svoje procedure sa ovim odredbama.

Cilj rada je da se omogući objedinjeni prikaz važećih bezbednosnih standarda, kao i odgovarajućih smernica za bezbednost u zdravstvu, čija primena omogućava veću bezbednost zaposlenih, pacijenata i drugih ljudi koji posećuju zdravstvene ustanove. Takođe, u radu će biti prikazani i regulatorni zahtevi koji se odnose na posebne kategorije podataka o ličnosti – podatke o zdravstvenom stanju.

Međunarodni i evropski standardi od značaja za bezbednost u zdravstvu

Jedan od krovnih nadnacionalnih standarda koji definiše oblast bezbednosti u zdravstvu jeste Uputstvo za menadžment bezbednosti u zdravstvenim ustanovama - CEN/TS 16850:2015. Ovaj evropski standard definiše zaštitu lica, kritičnih procesa, imovine i informacija od bezbednosnih pretnji i primenjuje se u bolnicama i drugim ustanovama koje pružaju zdravstvene usluge.

Pored toga što ističe značaj pravnih, regulatornih i drugih zahteva u vezi sa menadžmentom bezbednosti u zdravstvenim ustanovama, ovaj standard ukazuje na značaj identifikovanja zakonskih ograničenja za određene bezbednosne procedure i njihove posledice u vezi sa bezbednošću, što se posebno može reći za zakonske zahteve u oblasti zaštite podataka o ličnosti zaposlenih, kao i svih korisnika zdravstvenih usluga.[464] U navedenom smislu, posebno je važna odredba da bezbednosni menadžment u zdravstvenim ustanovama treba da bude usklađen sa drugim politikama i da poštuje prava pacijenata i posetilaca.

U vezi sa menadžmentom rizikom, ističe se da zdravstvena organizacija treba da uspostavi, implementira i održava formalne i dokumentovane procese procene rizika sa ciljem identifikovanja bezbednosnih rizika prouzrokovanih namernim i nenamernim pretnjama koje mogu izazvati direktne ili indirektne posledice po bezbednost, imovinu i zainteresovane strane.

Nadalje, politika bezbednosnog menadžmenta treba da sadrži ciljeve organizacije, što bi sa aspekta zaštite informacije značilo da se artikuliše jasna veza između zaštite informacija i ciljeva i politike organizacije, uključujući i politiku menadžmenta bezbednosti. Ne

[464] Ове процедуре су у већини случајева саставни део стандарда система менаџмента, нпр система менаџмента квалитетом

manje važno je da ciljevi organizacije u vezi sa zaštitom informacija budu dostupni i jasno predstavljeni svim zaposlenim u organizaciji, što će imati uticaj na sistem odgovornosti i posvećenost konkretnom cilju. Navedena politika treba dalje da se konkretizuje putem *plana menadžmenta bezbednosti*, a na osnovu procenjenih rizika. Takav plan bi trebalo posebno da obuhvati identifikaciju bezbednosno osetljivih tačaka i zona, pregled dužnosti i aktivnosti u vezi sa pretpostavljenim ciljevima bezbednosti, sistem dokumentacije (tj. evidencije i izveštaji), kao i programe obuke koji obuhvataju različite kategorije zaposlenog osoblja.

Od posebnog značaja za bezbednost informacija je povezivanje menadžmenta bezbednosti informacija sa drugim sistemima menadžmenta čime se menadžment bezbednosti informacija usklađuje sa sistemima menadžmenta kvalitetom, sistemom menadžmenta životnom sredinom itd.

Standard definiše operativno uputstvo i opšte procedure zdravstvene organizacije za kontrolisane zone kao prostore zaštićene od neovlašćenog pristupa, uključujući i konkretne sisteme za kontrolu pristupa, bezbedno skladištenje i čuvanje osetljivih i klasifikovanih informacija. U vezi sa tim, definisana su i operativna uputstva za bezbednosnu proveru lica, tj. personala, kojima se obezbeđuje usklađenost sa propisima u oblasti zaštite lica, imovine i informacija.

Kao posebne kategorije koje zahtevaju primenu bezbednosnih standarda i procedura, ovaj standard prepoznaje posetioce, pacijente, i, što je posebno važno, decu i njihovu bezbednost. U smislu zaštite informacija, podaci o deci mogu se ticati pitanja vezanih za moguće zlostavljanje dece, sporove oko starateljstva, deci kao žrtvama kriminalnih aktivnosti, uključujući i krijumčarenje.

Kada je reč o odgovoru na bezbednosni incident, definisani su kriterijumi šta se može smatrati bezbednosnim incidentom, između ostalog: gubitak, kompromitovanje ili zloupotreba osetljivih ili vitalnih informacija.

Evropska regulativa u oblasti zaštite informacija dobila je nov kvalitet donošenjem evorpskog standarda *SRPS EN 15224:2017 Zdravstvene usluge – Sistemi menadžmenta kvalitetom – Zahtevi zasnovani na SRPS EN ISO 9001:2015.* Ovaj standard, poznat i kao „ISO 9001 za zdravstvenu zaštitu“, između ostalog, stavlja akcenat na zdravstvenu zaštitu orijentisanu prema pacijentu, uključujući njegov fizički, psihološki i socijalni integritet.

U okviru bezbednosti zdravstvenih ustanova, u centru pažnje ovog standarda su, pored pacijenata i drugih korisnika zdravstvenih usluga, zaposleno osoblje, imovina i informacije. Kao poverljive (naročito osetljive) informacije smatraju se: lični podaci pacijenta/korisnika; podaci koji se odnose na zdravstveno stanje pacijenta; i podaci o dijagnostičkim procedurama i lečenju pacijenta. Sa aspekta zakonske regulative, ova materija je pokrivena propisima o zaštiti podataka ličnosti, o pravima pacijenta (pravo na privatnost i

poverljivost), itd. Zdravstvena ustanova mora imati uspostavljen sistem za zaštitu informacija o pacijentu od neovlašćenog pristupa i zloupotrebe.

Zaštita podataka o ličnosti u sistemu zdravstvene zaštite

Kada je Opšta uredba o zaštiti podataka Evropske unije (General Data Protection Regulation – GDPR, u daljem tekstu: Uredba) stupila na snagu 25. maja 2018. godine, izazvala je ozbiljne reakcije u različitim sektorima i industrijama širom sveta. Uredba postavlja novi standard u pogledu privatnosti podataka: utiče na bilo koju organizaciju koja obrađuje podatke građana EU, bez obzira gde se ti podaci prikupljaju, obrađuju ili čuvaju. Ovim regulativa dobija mnogo širi obim, proširujući domet na teritorije izvan EU i utičući na organizacije širom sveta, u bilo kojoj industriji. Za oblast zdravstvene zaštite, koja zahteva različite vrste ličnih podataka, to je prilika da se poboljšaju sistemi, politike i procesi kako bi se izbegle potencijalne pretnje za informacije o institucijama i pacijentima.

Prema odredbama evropske i važeće nacionalne regulative u Srbiji (Zakon o zaštiti podataka o ličnosti, "Sl. glasnik RS" br. 87/2018 od 13.11.2018.) podaci o zdravstvenom stanju spadaju u posebne vrste podataka o ličnosti, kojima su obuhvaćeni i genetski podaci i biometrijski podaci. Uredba generalno zabranjuje bilo kakvu obradu ovih podataka, osim ako nije dat izričiti pristanak ili nisu ispunjeni vrlo specifični uslovi. Postoje izuzeci - obrada je uglavnom dozvoljena za procenu radne sposobnosti za zapošljavanje, za upravljanje zdravstvenim sistemima ili sistemima socijalne zaštite i uslugama ili za javni interes.

Potrebno je istaći da su zdravstvene organizacije u specifičnoj poziciji, jer se bave čitavim spektrom podataka - od finansijskih podataka i informacija o zdravstvenom osiguranju do rezultata ispitivanja pacijenta i biometrijskih informacija. Neki od ovih vidova podataka su osetljiviji od tipičnih informacija koje prikupljaju nezdravstvene organizacije: one su jedinstveno povezane sa pojedincem i uglavnom su nepromenjive.

Upravljanje medicinskom dokumentacijom, koja sadrži posebno osetljive lične podatake, zahteva da su procesi monitoringa dizajnirani s posebnom pažnjom. Po pravilu, u zdravstvenim ustanovama primenjuje se dugi rok arhiviranja dokumenata. Što je duži rok čuvanja dokumentacije – proces je skuplji, složeniji, riskantniji i generalno zahtevniji. Dodatno, ovo nosi sa sobom potencijalni rizik: samo jedan izgubljeni (ili oštećeni, nedostupan ili prekasno dostupan) dokument može značiti razliku između uspeha i neuspeha u lečenju.

Zdravstvene ustanove, koje prema odredbama važeće regulative predstavljaju rukovaoce podacima o ličnosti, dužan da preduzme odgovarajuće tehničke, organizacione i kadrovske mere kako bi obezbedio da se obrada vrši u skladu sa propisanim odredbama. Potrebno je istaći da zakonodavac daje mogućnost da u primeni navedenih mera rukovalac podacima o ličnosti može uzeti u obzir nivo tehnoloških dostignuća i troškove njihove

primene, prirodu, obim, okolnosti i svrhu obrade, kao i verovatnoću nastupanja rizika i nivo rizika za prava i slobode fizičkih lica koji proizilaze iz obrade podataka o ličnosti.

Uredba jasno određuje individualnu odgovornost svake organizacije koja obrađuje podatke o ličnosti, što u praktičnom smislu znači da je dužnost svake organizacije da se samostalno pripremi za primenu Uredbe i uskladi svoje interne procese obrade podataka zahtevima Uredbe. Uredba određuje obavezu izvršenja takozvane „Procene uticaja obrade podataka" („Data Processing Impact Assessment") u situacijama kada se podaci vezani za zdravstveno stanje obrađuju u „velikom obimu". Dodatno, propisuje se obaveza ugovornog regulisanja odnosa i odgovornosti u vezi sa zaštitom ličnih podataka između organizacija koje su rukovaoci obrade i organizacija koje im pružaju uslugu spoljnje obrade podataka (eksterni isporučioci usluge), koji su u tom slučaju obrađivači podataka (npr. između klinike i dijagnostičke laboratorije koja za kliniku vrši uslugu).

Svaka organizacija je dužna samostalno da proceni koliki je obim posla potreban za usklađivanje sa odredbama regulative, imajući u vidu puno različitih faktora kao što su, na primer, kompleksnost obrade podataka kojom se organizacija bavi, broj individualnih korisnika usluga, veličina organizacije i slično.

Osnovne mere zaštite podataka o ličnosti u informacionim sistemima

Potrebno je istaći da je sama regulativa definisala neke od mere zaštite podataka o ličnosti u informacionim sistemima, kao što su enkripcija i pseudonimizacija. Takođe, druge, veoma korisne mere zaštite mogu imati svoju primenu: razdvanje zaduženja, kontrola pristupa dokumentima i podacima (na „*need to know*" osnovi), razmena podataka o ličnosti u skladu sa procenom rizika, obezbeđenje redundantosti da bi se izbegao „*single point of failure*", monitoring aktivnosti, uključujući privilegovane korisnike, kontrola spoljnjeg pristupa mrežama i razdvajanje mreža, učenje iz incidenata itd.

Pseudonimizovani podaci su podaci od kojih su uklonjene informacije pomoću kojih se osoba može identifikovati. Drugim rečima, podaci iz kojih se ne može nedvosmisleno utvrditi identitet osobe smatraju se pseudonimizovanim. Na primer, imena u tablici koja su zamenjena nasumičnim rečima/brojevima (identifikatorima) po ključu jedan za jedan. Podaci su i dalje tu i može se utvrditi da se radi o nekome, ali ne tačno i o kome.

To su i dalje podaci o ličnosti i ne smatraju se potpuno nerizičnima, ali rizik je znatno smanjen.

Druga mera koja je regulativom preporučena je enkripcija. Visokorizični podaci idealan su kandidat za enkripciju, i to tokom čitavog njihovog životnog ciklusa. To uključuje trenutak primanja podataka od korisnika, za šta se koriste mrežni kriptografski protokoli, obrade (enkripcija memorije) i naknadnog arhiviranja. Dobro zaštićeni podaci sami su po sebi sigurni, čak i u slučajevima povrede podataka, takvi su podaci korisnicima

neupotrebljivi. Iz tog razloga se kriptovanje u Zakonu o zaštiti podataka o ličnosti izričito navodi kao primer dobre prakse za zaštitu podataka.

Sigurnosnim kopijama štite se podaci koje organizacija može izgubiti usled malicioznih napada, slučajnog brisanja ili kvara na opremi. Sigurnosne kopije treba pripremati u skladu sa intervalima koje je zdravstvena organizacija propisala kao najpogodnije i redovno ih ažurirati, uz napomenu da sigurnosne kopije posebnih kategorija podataka o ličnosti treba raditi češće (i pažljivije). Po pravilu, sve kopije se čuvaju na sigurnom mestu s ograničenim pristupom, dok se medije treba čuvati na mestu koje odgovara njihovim radnim parametrima (vlažnost, temperatura, itd.).

Zaključak

U radu se daje objedinjeni prikaz važećih međunarodnih i evropskih bezbednosnih standarda, kao i odgovarajućih smernica za bezbednost u zdravstvu, čijom se primenom omogućava veća bezbednost zaposlenih, pacijenata i drugih ljudi koji posećuju zdravstvene ustanove.

Od posebnog značaja su i regulatorni zahtevi koji se odnose na posebne kategorije podataka o ličnosti – podatke o zdravstvenom stanju. Primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera zdravstvene organizacije će osigurati da su adekvatne politike i procedure za zaštitu podataka o ličnosti uspostavljene. Procesom implementacije i usaglašavanja sa odredbama Uredbe i nacionalne regulative u ovoj oblasti osiguraće se da su svi poslovni procesi detaljno preispitani, kao i da se unapredi upravljanje organizacijom.

Regulativa zahteva preduzimanje proporcionalnih mera u slučaju da dođe do povrede podataka o ličnosti, obaveštavanje odgovarajućih nadležnih organa, što će temeljna analiza sistema i procesa omogućiti da se izvrši u najboljoj mogućoj meri. Kada su kadrovske mere u pitanju, one podrazumevaju prethodnu detaljnu obuku svih zaposlenih, ali i uspostavljanje adekvatnih politika obrade podataka, koje treba da budu napisane razumljivim jezikom, i koje mogu biti dostupne u elektronskom obliku.

Literatura

1. Direktiva EU o kritičnim infrastrukturama (2008/114/ES)
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.
3. SRPS EN 15224:2017 Zdravstvene usluge – Sistemi menadžmenta kvalitetom
4. Uputstvo za menadžment bezbednosti u zdravstvenim ustanovama - CEN/TS 16850:2015.
5. Zakon o kritičnim infrastrukturama (Službeni glasnik RS", broj 87 od 13. novembra 2018.)
6. Zakon o zaštiti podataka o ličnosti, „Sl.glasnik Republike Srbije“, br. 87/2018 od 13.11.2018. godine