Analiza rizika informacione bezbednosti — Dr Tijana

Korisnik: Dr Tijana

Analizu pripremio: Biro za digitalnu bezbednost d.o.o.

POVERLJIVO I INTELEKTUALNA SVOJINA BDB — dokument firme „Dr Tijana“ sadrži analizu bezbednosnih rizika IKT sistema. Dokument se koristi isključivo za interne potrebe krajnjeg korisnika; neovlašćeno umnožavanje ili distribucija trećim licima nije dozvoljeno.

Datum izrade: 07.11.2026.

Sadržaj

- Uvod
- Metodologija procene rizika
- Nivoi rizika
- Nalazi po tematskim oblastima
- Upravljanje i organizaciona struktura
- Politike bezbednosti i klasifikacija
- Upravljanje pristupom i identitetima
- Prihvatljivo korišćenje i svest zaposlenih
- Tehnička zaštita mreže i sistema
- Upravljanje podacima i skladištenjem
- Monitoring i evidencije
- Cloud servisi i spoljni IT provajderi
- Reagovanje na incidente i oporavak
- Fizička bezbednost
- Odnos sa trećim stranama
- Licenciranje softvera i legalnost sistema
- Pregled nivoa rizika po oblastima
- Zaključak
- Prilozi

Uvod

Na osnovu Zakona o informacionoj bezbednosti („Sl. glasnik RS“, br. 91/2025), operator IKT sistema od posebnog značaja dužan je da izvrši procenu rizika i na osnovu nje izradi Akt o bezbednosti IKT sistema. Ova analiza predstavlja tu procenu rizika za „Dr Tijana“.

Dokument je izrađen primenom metodologije iz Pravilnika o opštoj metodologiji za procenu rizika u informaciono-komunikacionim sistemima od posebnog značaja („Sl. glasnik RS“, br. 63/2026), uz oslanjanje na međunarodno priznate okvire za upravljanje rizikom informacione bezbednosti — ISO/IEC 27001 i ISO/IEC 27005 — i smernice američkog Nacionalnog instituta za standarde i tehnologiju (NIST Cybersecurity Framework). Mere zaštite iz čl. 10 st. 4 Zakona na kojima se ova analiza oslanja sadržinski odgovaraju merama upravljanja sajber rizikom iz člana 21. Direktive (EU) 2022/2555 (NIS2), čime je obezbeđena usklađenost nalaza sa vodećim evropskim i globalnim standardima, nezavisno od toga što Republika Srbija nije članica EU.

Metodologija procene rizika

Za svaku pretnju iz Kataloga pretnji informacione bezbednosti izračunata je verovatnoća (na osnovu odgovora klijenta o postojećim merama zaštite) i uticaj (na osnovu kritičnosti pogođenih informacionih dobara iz registra resursa), prema formuli Vrednost rizika = Verovatnoća × Uticaj (opseg 1–25). Nalazi u nastavku grupisani su u 12 tematskih oblasti radi preglednosti rukovodstvu; kompletan registar po pojedinačnim pretnjama, GAP mapa usklađenosti sa čl. 10 Zakona i stavke za proveru dati su u prilogu.

Nivoi rizika

Nivo	Značenje
veoma nizak	Zanemarljiv uticaj na poslovanje; postojeće mere su adekvatne.
nizak	Ograničen uticaj; nije prioritet za hitno delovanje.
srednji	Umerena izloženost; potrebne su korektivne mere u razumnom roku.
visok	Značajna izloženost koja može ozbiljno ugroziti podatke ili procese; zahteva prioritetno delovanje.
veoma visok	Kritična izloženost koja može dovesti do ozbiljnog prekida rada ili trajnog gubitka podataka; zahteva hitnu intervenciju.

Nalazi po tematskim oblastima

Upravljanje i organizaciona struktura

Nivo rizika: veoma visok

Stanje: U [NAZIV FIRME] odgovornost za pojedinačne sisteme i procese je formalno definisana (§3.5), a ulogu praćenja usklađenosti i nadzora nad informacionom bezbednošću trenutno obavlja [IME ODGOVORNOG LICA], direktor i osnivač ordinacije. Međutim, zaposleni nemaju pisana uputstva za rad sa ključnim sistemima (§3.1), a u organizaciji ne

postoji formalno zadužena osoba ili tim za informacionu bezbednost (§3.17). U skladu sa tim, organizaciona struktura za upravljanje bezbednošću nije uspostavljena (tačka 1), nisu obezbeđeni dovoljni resursi za ovu funkciju (tačka 5), a status usvajanja relevantnih dokumenata je nejasan (tačka 36).

Pretnja: Odsustvo formalno zadužene osobe ili tima za informacionu bezbednost, u kombinaciji sa nepostojanjem pisanih uputstava za rad sa ključnim sistemima, znači da bezbednost sistema zavisi od ad-hoc postupanja pojedinaca i od ličnog angažovanja direktora, bez sistemskog nadzora. U uslovima kada je odgovornost koncentrisana na jednu osobu koja obavlja i upravljačku i operativnu ulogu (direktor), a nedostaju resursi i formalizovana struktura, rizik da se bezbednosni propusti ne uoče ili ne saniraju na vreme je veoma visok.

Preporuka: Potrebno je formalno imenovati osobu ili uspostaviti tim zadužen za informacionu bezbednost (čime se adresira §3.17 i tačka 1), uz jasno definisanje organizacione strukture i dodelu dovoljnih resursa (tačka 5) za obavljanje ove funkcije nezavisno od svakodnevnih operativnih obaveza direktora. Potrebno je izraditi i usvojiti pisana uputstva za rad sa ključnim sistemima za zaposlene (§3.1), kao i razjasniti i formalno usvojiti sva relevantna dokumenta iz oblasti informacione bezbednosti (tačka 36).

Uticaj na poslovanje: S obzirom na to da ključni poslovni proces — zakazivanje i vođenje medicinske dokumentacije pacijenata — zavisi od IKT sistema, materijalizacija ovog rizika bi direktno ugrozila kontinuitet pružanja zdravstvenih usluga i poverljivost osetljivih zdravstvenih podataka pacijenata. Nedostatak formalne strukture i uputstava povećava verovatnoću da se incident ne spreči, ne otkrije na vreme ili se neadekvatno sanira, što dodatno povećava pravne i reputacione posledice za ordinaciju.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 1 (Organizaciona struktura) — nije ispunjeno; tačka 5 (Dovoljno resursa) — nije ispunjeno; tačka 36 (Usvajanje dokumenata) — nejasno

Politike bezbednosti i klasifikacija

Nivo rizika: veoma visok

Stanje: U [NAZIV FIRME] ne postoji formalna politika klasifikacije informacija (org_5), iako su u praksi prepoznata dva neformalna nivoa osetljivosti — interno i poverljivo (klas_1), pri čemu se u najosetljiviju kategoriju svrstavaju medicinski kartoni pacijenata i kadrovski podaci zaposlenih (klas_2). Ova klasifikacija se, međutim, ne zasniva na pisanom pravilu niti formalnoj odluci — osetljivost podatka se prepoznaje intuitivno, po vrsti podatka, bez dokumentovane procedure ili određenog lica koje donosi tu odluku (klas_5). Ne postoje ni diferencirana pravila rukovanja po nivoima osetljivosti (klas_3), ni vizuelno obeležavanje dokumenata stepenom poverljivosti, poput oznake „POVERLJIVO" (klas_4). Dodatno, pravila o načinu deljenja osetljivih podataka putem imejla ili štampe su potpuno nedefinisana (§3.9).

Pretnja: Odsustvo formalne klasifikacije i pravila rukovanja (org_5, klas_3, klas_4, §3.9) znači da zaposleni nemaju jasne smernice kada i kako smeju deliti, štampati ili prosleđivati medicinske kartone i kadrovske podatke, što povećava verovatnoću nenamernog otkrivanja ili nekontrolisanog oticanja osetljivih zdravstvenih podataka. Pošto ne postoji ni formalizovana odluka o tome ko klasifikuje podatke (klas_5), odgovornost za eventualni propust ostaje nejasna, a sistem zavisi isključivo od individualne procene zaposlenih. Imajući u vidu prirodu podataka (medicinski kartoni pacijenata), ovaj rizik je direktno povezan sa merama iz tačke 8 (klasifikacija podataka) i tačke 14 (zaštita od oticanja podataka) čl. 10 Zakona, koje trenutno nisu ispunjene.

Preporuka: Potrebno je doneti pisanu politiku klasifikacije informacija koja formalizuje postojeće nivoe (interno, poverljivo), eksplicitno definiše da medicinski kartoni i kadrovski podaci spadaju u najviši nivo poverljivosti, i odredi lice (predlog: direktor, [IME ODGOVORNOG LICA]) odgovorno za donošenje i dokumentovanje odluka o klasifikaciji. Politika treba da propiše konkretna pravila rukovanja za svaki nivo — način deljenja putem imejla, uslove štampanja, čuvanja i uništavanja dokumenata — kao i obavezno vizuelno obeležavanje poverljivih dokumenata (npr. zaglavlje „POVERLJIVO"). Ovim bi se istovremeno adresirale mere iz tačke 8 (klasifikacija podataka) i tačke 14 (zaštita od oticanja podataka) čl. 10 Zakona.

Uticaj na poslovanje: Materijalizacija ovog rizika bi direktno ugrozila poverljivost zdravstvenih podataka pacijenata, što za ordinaciju predstavlja kršenje osnovne obaveze čuvanja medicinske tajne i izlaže je pravnim i reputacionim posledicama. S obzirom da zakazivanje i vođenje medicinske dokumentacije predstavljaju ključni poslovni proces, neovlašćeno otkrivanje ili curenje podataka moglo bi direktno narušiti poverenje pacijenata i sposobnost pružanja zdravstvenih usluga.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 8 (Klasifikacija podataka) — nije ispunjeno; tačka 14 (Zaštita od oticanja podataka) — nije ispunjeno

Upravljanje pristupom i identitetima

Nivo rizika: veoma visok

Stanje: U [NAZIV FIRME] nije definisano da li se pristup podacima dodeljuje isključivo zaposlenima kojima je neophodan za obavljanje posla (§3.16), niti je uspostavljena višefaktorska autentikacija za pristup ključnim sistemima (§4.3). Ne postoji periodična provera dodeljenih prava pristupa niti uklanjanje nepotrebnih ovlašćenja (§4.4), a nije definisano ni postoji li kontrola koja sprečava neovlašćenu izmenu ili otkrivanje ključnih podataka (§4.10/4.12). Procedura za hitno oduzimanje pristupa zaposlenom koji napušta firmu ili menja poziciju nije definisana (§6.1), a rad na daljinu nije zaštićen odgovarajućim merama poput VPN-a, enkriptovane komunikacije ili kontrole pristupa sa udaljenih uređaja (§4.21). Pozitivno je što je pristup podešavanjima sistema ograničen na ovlašćene administratore (§4.2) i što su lozinke lične, bez deljenja naloga (§4.7).

Pretnja: Nepostojanje kontrole ko ima pristup kojim podacima, odsustvo MFA i neadekvatna zaštita rada na daljinu značajno povećavaju verovatnoću neovlašćenog pristupa medicinskoj dokumentaciji pacijenata, bilo od strane internog lica sa prekomernim ovlašćenjima, bivšeg zaposlenog čiji pristup nije blagovremeno ukinut, ili eksternog napadača koji iskoristi nezaštićenu udaljenu vezu. S obzirom na to da firma posluje u zdravstvenom sektoru i obrađuje posebno osetljive podatke o pacijentima, ovakvi propusti predstavljaju direktan rizik od neovlašćenog otkrivanja, izmene ili gubitka integriteta medicinskih podataka.

Preporuka: Potrebno je uspostaviti jasnu politiku dodele pristupa po principu nužnog znanja (least privilege) i uvesti redovnu, najmanje polugodišnju reviziju korisničkih prava uz uklanjanje nepotrebnih ovlašćenja. Treba uvesti višefaktorsku autentikaciju za pristup sistemima koji sadrže medicinsku dokumentaciju, definisati formalnu proceduru za hitno oduzimanje pristupa pri prestanku radnog odnosa ili promeni pozicije, kao i implementirati bezbedan VPN i enkriptovanu komunikaciju za rad na daljinu. Dodatno je neophodno jasno definisati i dokumentovati kontrole koje sprečavaju neovlašćenu izmenu ili otkrivanje ključnih podataka. U skladu sa GAP listom iz čl. 10 Zakona, potrebno je otkloniti neispunjene mere koje se odnose na bezbednost rada na daljinu (tačka 3), ograničenje pristupa (tačka 10) i zaštitu od oticanja podataka (tačka 14), dok je potrebno dodatno razjasniti i formalizovati mere koje se odnose na zaštitu pri promeni poslova zaposlenih (tačka 6), odgovornost korisnika (tačka 12) i multifaktorsku autentifikaciju (tačka 37).

Uticaj na poslovanje: Materijalizacija ovog rizika mogla bi da ugrozi poverljivost i integritet zdravstvenih podataka pacijenata i direktno naruši sposobnost ordinacije da nesmetano obavlja zakazivanje i vođenje medicinske dokumentacije, što predstavlja ključni poslovni proces. Osim operativnog prekida u pružanju zdravstvenih usluga, posledice bi uključivale gubitak poverenja pacijenata i izloženost pravnoj i regulatornoj odgovornosti zbog neadekvatne zaštite osetljivih ličnih podataka.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 3 (Bezbednost rada na daljinu) — nije ispunjeno; tačka 6 (Zaštita pri promeni poslova zaposlenih) — nejasno; tačka 10 (Ograničenje pristupa) — nije ispunjeno; tačka 12 (Odgovornost korisnika) — nejasno; tačka 14 (Zaštita od oticanja podataka) — nije ispunjeno; tačka 37 (Multifaktorska autentifikacija) — nejasno

Prihvatljivo korišćenje i svest zaposlenih

Nivo rizika: visok

Stanje: U [NAZIV FIRME] politika o dozvoljenom korišćenju IT opreme i interneta nije definisana (§4.5). Kontrola USB portova i prenosivih medijuma je uspostavljena i ocenjena kao zadovoljavajuća (§2.9). Zaposleni ne prolaze obuku iz informacione bezbednosti (§3.15) i nisu osposobljeni da prepoznaju socijalni inženjering, poput lažnih poziva ili fišing napada (§4.19).

Pretnja: Odsustvo politike prihvatljivog korišćenja i neobučenost zaposlenih za prepoznavanje socijalnog inženjeringa stvaraju visok rizik da zaposleni, bez jasnih smernica i svesti o pretnjama, nenamerno omoguće neovlašćen pristup IKT sistemima ili kompromitaciju osetljivih podataka. S obzirom na to da se u ordinaciji obrađuju zdravstveni podaci pacijenata, ovakav propust povećava verovatnoću uspešnog napada putem fišinga ili socijalnog inženjeringa koji bi mogao dovesti do neovlašćenog pristupa medicinskoj dokumentaciji.

Preporuka: Potrebno je doneti i formalizovati politiku o dozvoljenom korišćenju IT opreme i interneta, koja jasno definiše obaveze i odgovornosti zaposlenih (čl. 10 tačka 12 Zakona), kao i uspostaviti redovan program obuke iz informacione bezbednosti za sve zaposlene, uključujući specifičnu obuku za prepoznavanje socijalnog inženjeringa i fišinga (čl. 10 tačka 4 Zakona). Obuke treba sprovoditi periodično, uz evidentiranje prisustva i provere usvojenog znanja, kako bi se osigurala stvarna osposobljenost korisnika sistema. Direktor, kao lice odgovorno za nadzor nad informacionom bezbednošću, treba da inicira i odobri navedene mere.

Uticaj na poslovanje: Materijalizacija ovog rizika mogla bi dovesti do neovlašćenog pristupa medicinskoj dokumentaciji pacijenata, narušavanja poverljivosti osetljivih zdravstvenih podataka i prekida ključnih procesa zakazivanja i vođenja dokumentacije. Ovo bi direktno ugrozilo sposobnost ordinacije da pruža zdravstvene usluge, uz moguće pravne i reputacione posledice usled kršenja propisa o zaštiti podataka o ličnosti.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 4 (Osposobljenost lica koja koriste sistem) — nije ispunjeno; tačka 12 (Odgovornost korisnika) — nejasno

Tehnička zaštita mreže i sistema

Nivo rizika: visok

Stanje: U [NAZIV FIRME] ne postoji provera „drugog para očiju" za kritične IT izmene (§3.2), a nije definisano ni da li se podešavanja sistema proveravaju pre puštanja u rad (§3.4), niti da li se izmene prethodno testiraju pre primene na produkcionom sistemu (§3.11). Ne prati se iskorišćenost kapaciteta sistema (§3.12), ne postoje mere specifično usmerene protiv ransomver napada poput nepromenljivih kopija i segmentacije mreže (§4.18), a nejasan je status ažurnosti i zaštite mrežnih štampača i skenera (§4.20). Dodatno, nije razmatran rizik od budućeg probijanja postojeće enkripcije kvantnim računarstvom (§2.8). Pozitivno je što se softver i operativni sistemi redovno ažuriraju (§3.10) i što je na svim uređajima prisutna zaštita od zlonamernog softvera (§3.6/4.6).

Pretnja: Nedostatak kontrole izmena i testiranja pre produkcije (§3.2, §3.4, §3.11) povećava verovatnoću da greška ili zlonamerna izmena ostane neotkrivena i izazove prekid rada kritičnih sistema. Odsustvo mera protiv ransomvera (§4.18) i nepraćenje kapaciteta sistema (§3.12) znatno uvećavaju rizik od uspešnog napada šifrovanjem podataka i produženog prekida rada bez mogućnosti blagovremenog upozorenja na preopterećenje

resursa. Nezaštićeni ili neažurirani mrežni uređaji (§4.20) predstavljaju dodatnu ulaznu tačku za napadače, dok neadresiran rizik postkvantne kriptografije (§2.8) ugrožava dugoročnu poverljivost osetljivih zdravstvenih podataka.

Preporuka: Potrebno je uvesti formalni proces odobravanja i nezavisne provere kritičnih IT izmena, uz obaveznu proveru konfiguracija i testiranje u izolovanom okruženju pre puštanja u produkciju. Treba implementirati mere specifične za zaštitu od ransomvera, uključujući nepromenljive (immutable) rezervne kopije i segmentaciju mreže, kao i uspostaviti redovno praćenje iskorišćenosti kapaciteta sistema. Neophodno je proveriti i dokumentovati bezbednosni status svih mrežnih štampača i skenera (ažuriranost, zaštita lozinkom), te započeti procenu izloženosti postojećih kriptografskih rešenja riziku kvantnog računarstva. U vezi sa GAP listom iz čl. 10 Zakona, treba uspostaviti kriptografske kontrole (tačka 13) i mehanizme zaštite od gubitka podataka (tačka 16), uvesti sistematsko praćenje sistema (tačka 19) i ograničenje pristupa veb prezentacijama (tačka 20), razjasniti i dokumentovati zaštitu od zloupotrebe poznatih slabosti (tačka 25), uspostaviti zaštitu pri revizorskom testiranju (tačka 26), jasno definisati zaštitu podataka u mrežama i bezbednost podataka u komunikaciji (tačke 27 i 28), uvesti bezbednosne zahteve tokom celog životnog ciklusa sistema (tačka 29) i formalizovati mere prevencije incidenata (tačka 34).

Uticaj na poslovanje: S obzirom na to da ključni poslovni proces — zakazivanje i vođenje medicinske dokumentacije pacijenata — u potpunosti zavisi od IKT sistema, materijalizacija ovih rizika mogla bi direktno onemogućiti pružanje zdravstvenih usluga. Dodatno, kompromitovanje ili gubitak osetljivih zdravstvenih podataka pacijenata predstavljao bi ozbiljno kršenje poverljivosti sa pravnim i reputacionim posledicama za [NAZIV FIRME].

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 13 (Kriptografske kontrole) — nije ispunjeno; tačka 16 (Zaštita od gubitka) — nije ispunjeno; tačka 19 (Praćenje sistema) — nije ispunjeno; tačka 20 (Ograničenje pristupa veb prezentacijama) — nije ispunjeno; tačka 25 (Zaštita od zloupotrebe slabosti) — nejasno; tačka 26 (Zaštita pri revizorskom testiranju) — nije ispunjeno; tačka 27 (Zaštita podataka u mrežama) — nejasno; tačka 28 (Bezbednost podataka u komunikaciji) — nejasno; tačka 29 (Zahtevi tokom životnog ciklusa) — nije ispunjeno; tačka 34 (Prevencija incidenata) — nije ispunjeno

Upravljanje podacima i skladištenjem

Nivo rizika: visok

Stanje: [NAZIV FIRME] primenjuje osnovne kontrole nad integritetom podataka — postoji kontrola verzija odnosno potvrda pre trajnih izmena važnih podataka (§3.7) i redovno se izrađuju rezervne kopije (§3.8). Međutim, utvrđeno je da osetljivi podaci nisu enkriptovani i da se ne testira uspešnost obnavljanja rezervnih kopija (§3.20/3.21), da se podaci ne brišu nepovratno po isteku propisanog ili ugovorenog roka čuvanja (§3.23), kao i da rezervne kopije nisu zaštićene od brisanja sa kompromitovanog naloga, odnosno nisu odvojene ili offline (§4.11). Dodatno, u pogledu mera iz čl. 10 Zakona, nisu ispunjene kriptografske kontrole (tačka 13), zaštita od gubitka podataka (tačka 16) i procedure čuvanja i brisanja

(tačka 31), dok je status ispravnosti sredstava za obradu podataka (tačka 17) i zaštite test podataka (tačka 30) nejasan.

Pretnja: Kombinacija neenkriptovanih osetljivih podataka, netestiranih rezervnih kopija i njihove izloženosti brisanju sa kompromitovanog naloga znači da u slučaju napada (npr. ransomware) ili tehničkog kvara ne postoji pouzdan mehanizam oporavka, a curenje podataka bi bilo neposredno čitljivo napadaču. Izostanak procedura za nepovratno brisanje po isteku roka čuvanja (§3.23) dodatno povećava izloženost usled nepotrebnog čuvanja osetljivih zdravstvenih podataka duže nego što je propisano ili ugovoreno. Nejasan status ispravnosti sredstava za obradu (tačka 17) i zaštite test podataka (tačka 30) ukazuje da rizik može biti i veći od evidentiranog, jer ovi aspekti nisu pouzdano proverjeni.

Preporuka: Potrebno je uvesti enkripciju osetljivih podataka, kako u mirovanju tako i pri prenosu (tačka 13), i uspostaviti redovno testiranje uspešnosti obnavljanja rezervnih kopija. Rezervne kopije treba fizički ili logički odvojiti (offline ili immutable skladište) tako da ne mogu biti izbrisane sa kompromitovanog naloga (§4.11, tačka 16). Treba definisati i primeniti pisanu proceduru čuvanja i nepovratnog brisanja podataka po isteku propisanog ili ugovorenog roka (§3.23, tačka 31), a zatim razjasniti i formalizovati status ispravnosti sredstava za obradu (tačka 17) i zaštite test podataka (tačka 30).

Uticaj na poslovanje: S obzirom da je ključni proces vođenje medicinske dokumentacije pacijenata, materijalizacija ovog rizika bi direktno ugrozila mogućnost pružanja zdravstvenih usluga i poverljivost osetljivih zdravstvenih podataka pacijenata, uz mogući gubitak podataka bez mogućnosti oporavka. Ovo nosi i regulatorne posledice s obzirom na prirodu podataka u zdravstvenom sektoru, kao i rizik od gubitka poverenja pacijenata.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 13 (Kriptografske kontrole) — nije ispunjeno; tačka 16 (Zaštita od gubitka) — nije ispunjeno; tačka 17 (Ispravnost sredstava) — nejasno; tačka 30 (Zaštita test podataka) — nejasno; tačka 31 (Procedure čuvanja i brisanja) — nije ispunjeno

Monitoring i evidencije

Nivo rizika: visok

Stanje: U [NAZIV FIRME] evidencije (logovi) o aktivnostima u IKT sistemima se ne čuvaju niti proveravaju redovno (§3.3), ne postoji mehanizam za uočavanje neuobičajene aktivnosti niti plan za slučaj prestanka rada ključnog sistema (§3.18/3.19), a postojeće evidencije nisu zaštićene od izmene ili brisanja od strane neovlašćenih lica (§4.1). U skladu sa tim, neispunjene su mere iz čl. 10 Zakona koje se odnose na prikupljanje podataka o pretnjama (tačka 2), praćenje sistema (tačka 19), čuvanje podataka o događajima (tačka 23) i kontinuitet poslova (tačka 35).

Pretnja: Bez redovnog nadzora i zaštićenih evidencija, neovlašćeni pristup medicinskoj dokumentaciji pacijenata ili zloupotreba sistema za zakazivanje mogli bi ostati neotkriveni duži vremenski period, a tragovi takvog incidenta mogli bi biti izmenjeni ili uništeni.

Odsustvo plana za slučaj prestanka rada ključnog sistema znači da bi ispad sistema za vođenje medicinske dokumentacije direktno zaustavio mogućnost pružanja zdravstvenih usluga, bez jasno definisanog načina oporavka.

Preporuka: Potrebno je uspostaviti redovno prikupljanje, čuvanje i periodičnu proveru evidencija (logova) o aktivnostima u sistemima koji obrađuju podatke pacijenata, uz tehničku zaštitu tih evidencija od neovlašćene izmene ili brisanja (npr. ograničavanjem prava pristupa i čuvanjem na odvojenoj lokaciji). Potrebno je definisati mehanizam za prikupljanje podataka o pretnjama i praćenje sistema radi blagovremenog uočavanja neuobičajene aktivnosti, kao i izraditi plan kontinuiteta poslovanja koji pokriva scenario prestanka rada ključnog sistema za zakazivanje i vođenje medicinske dokumentacije. Odgovornost za sprovođenje i praćenje ovih mera treba formalno dodeliti, u skladu sa ulogom direktora u nadzoru nad informacionom bezbednošću.

Uticaj na poslovanje: Materijalizacija ovog rizika bi ugrozila poverljivost i integritet osetljivih zdravstvenih podataka pacijenata, a nemogućnost blagovremenog otkrivanja incidenta ili oporavka ključnog sistema direktno bi onemogućila zakazivanje i pružanje zdravstvenih usluga. Ovo nosi reputacioni rizik i rizik od narušavanja zakonskih obaveza u pogledu zaštite zdravstvenih podataka, uz mogući prekid poslovnih procesa ordinacije.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 2 (Prikupljanje podataka o pretnjama) — nije ispunjeno; tačka 19 (Praćenje sistema) — nije ispunjeno; tačka 23 (Čuvanje podataka o događajima) — nije ispunjeno; tačka 35 (Kontinuitet poslova) — nije ispunjeno

Cloud servisi i spoljni IT provajderi

Nivo rizika: veoma visok

Stanje: U [NAZIV FIRME] angažovanje spoljnih IT provajdera i cloud servisa nije ugovorno regulisano na adekvatan način — postupanje po zahtevu državnih organa i podrška u slučaju incidenta nisu definisani (§5.5/5.8), a sa provajderima ne postoji potpisan ugovor koji reguliše obradu ličnih podataka (§5.7). Dodatno, zaposleni nisu upoznati sa rizicima AI-generisanih prevara, niti je zaštićen unos podataka u AI alate (§5.9/5.10). U skladu sa tim, više tačaka iz čl. 10 Zakona je neispunjeno ili nejasno definisano: osposobljenost lica koja koriste sistem (tačka 4), zaštita od oticanja podataka (tačka 14), procedure čuvanja i brisanja (tačka 31) i prevencija incidenata (tačka 34) nisu ispunjene, dok su procedure za računarstvo u klaudu (tačka 18), zaštita sredstava dostupnih pružaocima (tačka 32) i održavanje ugovorenog nivoa usluge (tačka 33) ocenjene kao nejasne.

Pretnja: Nepostojanje ugovorne osnove za obradu ličnih podataka i postupanje u slučaju incidenta znači da [NAZIV FIRME] nema pravnu niti operativnu garanciju da će provajder adekvatno reagovati u slučaju bezbednosnog incidenta ili zahteva državnog organa, niti da će medicinski podaci pacijenata biti zaštićeni u skladu sa zakonom. Nejasne procedure za cloud (tačka 18, 32, 33) i nedostatak prevencije incidenata (tačka 34) povećavaju verovatnoću da propust provajdera ostane neotkriven ili nerešen, dok neosposobljenost

zaposlenih (tačka 4) i nekontrolisano korišćenje AI alata (§5.9/5.10) stvaraju dodatni kanal oticanja osetljivih podataka (tačka 14) mimo nadzora ordinacije.

Preporuka: Potrebno je hitno zaključiti ili dopuniti ugovore sa svim cloud i IT provajderima tako da eksplicitno regulišu obradu ličnih podataka, postupanje po zahtevima državnih organa, podršku u slučaju incidenta i nivo usluge (SLA), čime bi se adresirale tačke 18, 31, 32, 33 i 34. Paralelno treba uspostaviti internu proceduru i obuku zaposlenih o bezbednom korišćenju cloud servisa i AI alata, uključujući zabranu unosa podataka pacijenata u nezaštićene AI sisteme, čime se pokriva tačka 4 i rizik oticanja podataka (tačka 14). Direktor, kao odgovorno lice, treba da inicira reviziju svih postojećih ugovora sa provajderima u narednom periodu.

Uticaj na poslovanje: S obzirom na to da ključni proces — zakazivanje i vođenje medicinske dokumentacije pacijenata — zavisi od IKT sistema i cloud infrastrukture, materijalizacija ovog rizika bi direktno ugrozila mogućnost pružanja zdravstvenih usluga i dovela do kompromitacije poverljivih zdravstvenih podataka pacijenata. Ovo bi moglo rezultovati prekidom rada ordinacije, gubitkom poverenja pacijenata i pravnim posledicama zbog neusklađenosti sa propisima o zaštiti podataka u zdravstvenom sektoru.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 4 (Osposobljenost lica koja koriste sistem) — nije ispunjeno; tačka 14 (Zaštita od oticanja podataka) — nije ispunjeno; tačka 18 (Procedure za računarstvo u klaudu) — nejasno; tačka 31 (Procedure čuvanja i brisanja) — nije ispunjeno; tačka 32 (Zaštita sredstava dostupnih pružaocima) — nejasno; tačka 33 (Održavanje ugovorenog nivoa usluge) — nejasno; tačka 34 (Prevencija incidenata) — nije ispunjeno

Reagovanje na incidente i oporavak

Nivo rizika: visok

Stanje: U [NAZIV FIRME] postoji procedura za prijavu gubitka ili krađe opreme (§3.13), kao i rezervna internet/telekom veza u slučaju otkaza primarne (§2.5). Međutim, ne postoji zamena za ključne IT uloge u slučaju odsustva (§3.14), ne postoji plan oporavka u slučaju velike prirodne nepogode (§1.4), a status rezervne opreme ili plana za slučaj kvara ključnog hardvera/softvera je nedefinisan (§2.4). U skladu sa tim, mere iz čl. 10 Zakona koje se odnose na zaštitu od gubitka (tačka 16) i kontinuitet poslova (tačka 35) nisu ispunjene.

Pretnja: Nepostojanje plana oporavka od katastrofe, nejasan status rezervne opreme i odsustvo zamene za ključne IT uloge znače da bi u slučaju ozbiljnog incidenta, kvara ili odsustva ključnog kadra, [NAZIV FIRME] mogla ostati bez mogućnosti da obnovi rad IKT sistema u razumnom roku. S obzirom da je ključni proces zakazivanje i vođenje medicinske dokumentacije pacijenata, svaki duži prekid direktno ugrožava kontinuitet pružanja zdravstvenih usluga i dostupnost osetljivih zdravstvenih podataka.

Preporuka: Potrebno je izraditi i formalizovati plan kontinuiteta poslovanja i oporavka od katastrofe (uključujući scenario prirodne nepogode), koji definiše postupke, odgovornosti i

rokove za obnovu rada ključnih IKT sistema. Neophodno je jasno definisati i dokumentovati rešenje za rezervnu opremu odnosno plan za slučaj kvara ključnog hardvera/softvera, kao i odrediti zamenu ili eksternog saradnika za ključne IT uloge za slučaj odsustva odgovornog lica. Ove mere direktno adresiraju neispunjene tačke 16 (Zaštita od gubitka) i 35 (Kontinuitet poslova) iz čl. 10 Zakona.

Uticaj na poslovanje: Materijalizacija ovog rizika bi dovela do prekida u zakazivanju pregleda i pristupu medicinskoj dokumentaciji pacijenata, čime bi bilo direktno ugroženo pružanje zdravstvenih usluga. Dodatno, produženi oporavak bez definisanih procedura i zamenskog kadra povećava rizik od trajnog gubitka podataka i narušavanja poverenja pacijenata, kao i mogućih regulatornih posledica zbog ugrožene poverljivosti zdravstvenih podataka.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 16 (Zaštita od gubitka) — nije ispunjeno; tačka 35 (Kontinuitet poslova) — nije ispunjeno

Fizička bezbednost

Nivo rizika: visok

Stanje: [NAZIV FIRME] ima uspostavljene mere zaštite okruženja u kojem se nalazi IT oprema — funkcionalan sistem za detekciju i gašenje požara (§1.1), zaštitu od prodora vode (§1.2), klimatizaciju i kontrolu vlage/prašine (§1.3), redovno nadgledanje temperature i vlažnosti (§2.1), rezervno napajanje putem UPS-a/agregata (§2.2) i zaštitu od elektromagnetnih smetnji (§2.3). Međutim, prostorije sa opremom nisu fizički obezbeđene odgovarajućim bravama, alarmnim sistemom niti video nadzorom (§4.14/4.16/4.17), što predstavlja ozbiljan nedostatak u kontroli fizičkog pristupa.

Pretnja: Nepostojanje fizičke zaštite prostorija sa opremom (§4.14/4.16/4.17) znači da neovlašćena lica mogu steći direktan fizički pristup serverima i uređajima na kojima se čuva medicinska dokumentacija pacijenata, bez mehanizma detekcije ili odvraćanja. U odsustvu brava, alarma i video nadzora, krađa opreme, neovlašćeno kopiranje ili uništavanje podataka mogli bi proći neopaženo, a tragovi za naknadnu istragu incidenta ne bi postojali.

Preporuka: Potrebno je hitno uvesti kontrolu fizičkog pristupa prostorijama sa opremom — ugradnju odgovarajućih brava (po mogućstvu sa evidencijom pristupa), alarmnog sistema koji reaguje na neovlašćen ulazak van radnog vremena, i video nadzora sa snimanjem ulaza u te prostorije. Istovremeno treba formalizovati i dokumentovati mere fizičke zaštite objekata (tačka 15 čl. 10 Zakona) i mere zaštite od gubitka podataka/opreme (tačka 16 čl. 10 Zakona), jer su obe trenutno neispunjene, uz određivanje lica odgovornog za upravljanje pristupom i periodičnu proveru funkcionisanja ovih mera.

Uticaj na poslovanje: Materijalizacija ovog rizika u zdravstvenoj ordinaciji mogla bi dovesti do fizičkog gubitka ili kompromitovanja opreme koja sadrži osetljive zdravstvene podatke pacijenata, čime bi bio direktno ugrožen proces zakazivanja i vođenja medicinske dokumentacije. Pored prekida pružanja zdravstvenih usluga, posledice bi uključivale

povredu poverljivosti podataka o pacijentima, narušavanje poverenja korisnika usluga i potencijalnu regulatornu odgovornost zbog neispunjenih zakonskih mera fizičke zaštite.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 15 (Fizička zaštita objekata) — nije ispunjeno; tačka 16 (Zaštita od gubitka) — nije ispunjeno

Odnos sa trećim stranama

Nivo rizika: nema podataka

Stanje: U [NAZIV FIRME] odnos sa trećim stranama (spoljni IT saradnik, eksterna laboratorija, dobavljač softvera za zakazivanje) upravlja se neformalno, kroz lični kontakt i dugogodišnju saradnju, bez pisanog procesa (§tr_1). Bezbednosna provera dobavljača ne sprovodi se ni pre potpisivanja ugovora (§vst_1), ni nakon njega (§tr_2), a postojeći dobavljači se nikada formalno ne proveravaju ponovo (§vst_4). Za nove saradnike se primenjuje samo referentna provera i ugovorne klauzule o poverljivosti (§vst_2), dok je uređenost obaveštavanja o bezbednosnim incidentima u ugovorima nejasna (§tr_3, §vst_3), kao i ograničavanje pristupa dobavljača internim sistemima na najmanju potrebnu meru i vreme (§vst_6). Ne postoji formalna procedura za raskid saradnje koja bi obuhvatala opoziv pristupa i povraćaj ili brisanje podataka (§vst_5), a u Aktu o bezbednosti je kao nejasna evidentirana i mera iz čl. 10 tačka 32 — Zaštita sredstava dostupnih pružaocima.

Pretnja: Bez formalne provere i ugovornog uređenja odnosa sa trećim stranama, spoljni saradnici i dobavljači mogu imati neograničen ili dugotrajno zadržan pristup sistemima i medicinskim podacima pacijenata i nakon prestanka potrebe za tim pristupom. Nejasna ili nepostojeća obaveza obaveštavanja o incidentima kod dobavljača znači da bi [NAZIV FIRME] mogla kasno ili uopšte ne saznati za bezbednosni događaj nastao kod treće strane koji ugrožava njene sisteme ili podatke. Nedostatak procedure za raskid saradnje dodatno povećava rizik da bivši saradnici zadrže pristup nakon prestanka ugovora.

Preporuka: Potrebno je uvesti pisanu proceduru za upravljanje trećim stranama koja obuhvata bezbednosnu proveru pre potpisivanja ugovora, periodičnu ponovnu proveru postojećih dobavljača i jasno definisane ugovorne klauzule o obaveštavanju o bezbednosnim incidentima u određenom roku. Potrebno je takođe formalizovati ograničavanje pristupa dobavljača na princip najmanjeg potrebnog obima i vremena, uspostaviti proceduru za raskid saradnje koja uključuje opoziv pristupa i povraćaj ili brisanje podataka, kao i razjasniti i dokumentovati primenu mere iz čl. 10 tačka 32 — Zaštita sredstava dostupnih pružaocima. Odgovornost za sprovođenje ovih mera treba dodeliti [IME ODGOVORNOG LICA] kao licu zaduženom za praćenje usklađenosti.

Uticaj na poslovanje: S obzirom na to da ključni poslovni proces zakazivanja i vođenja medicinske dokumentacije direktno zavisi od eksternih saradnika i dobavljača, bezbednosni incident nastao kod treće strane mogao bi direktno ugroziti kontinuitet pružanja zdravstvenih usluga i poverljivost osetljivih zdravstvenih podataka pacijenata. Nivo rizika za ovu oblast nije utvrđen dostupnim podacima, ali evidentirani nedostaci ukazuju na izloženost koja zahteva dalju procenu i hitno uređenje ugovornih i proceduralnih kontrola.

Mere iz čl. 10 st. 4 Zakona relevantne za ovu oblast (vidi i Akt o bezbednosti): tačka 32 (Zaštita sredstava dostupnih pružaocima) — nejasno

Licenciranje softvera i legalnost sistema

Nivo rizika: nizak

Stanje: Prema odgovoru na pitanje šifre 4.13, u [NAZIV FIRME] se softver preuzima isključivo iz pouzdanih, zvaničnih izvora, čime je ova praksa ocenjena kao uspostavljena. Na osnovu dostavljenih dokaza, izračunata verovatnoća i uticaj za ovaj nalaz su niski, što rezultira niskim nivoom rizika u oblasti licenciranja softvera i legalnosti sistema. Drugi aspekti ove oblasti (npr. formalna evidencija licenci, periodična provera legalnosti instaliranog softvera) nisu obuhvaćeni dostavljenim dokazima, te se o njima ne iznosi ocena.

Pretnja: I pored uspostavljene prakse preuzimanja softvera iz zvaničnih izvora, preostali rizik se odnosi na mogućnost da pojedinačni propust ili nenamerno preuzimanje softvera iz nepouzdanog izvora dovede do unošenja malicioznog koda u sistem. S obzirom da ključni poslovni proces — zakazivanje i vođenje medicinske dokumentacije pacijenata — zavisi od IKT sistema, ovakav scenario bi mogao ugroziti dostupnost i integritet osetljivih zdravstvenih podataka. Nivo rizika je, prema datoj metodologiji, nizak, ali ne i nepostojeći.

Preporuka: Preporučuje se da [NAZIV FIRME] formalizuje postojeću praksu preuzimanja softvera isključivo iz zvaničnih izvora kroz internu pisanu smernicu ili uputstvo, kako bi se obezbedila dosledna primena i u slučaju promene odgovornog lica. Dodatno, preporučuje se periodična provera legalnosti i porekla instaliranog softvera na svim radnim stanicama i serverima koji učestvuju u obradi medicinske dokumentacije. Odgovornost za sprovođenje i nadzor ove preporuke treba da ostane kod direktora, [IME ODGOVORNOG LICA], kao lica zaduženog za usklađenost sa propisima o informacionoj bezbednosti.

Uticaj na poslovanje: Ukoliko bi se rizik materijalizovao, na primer putem malicioznog softvera unetog preko nepouzdanog izvora, posledica bi mogla biti ugrožavanje dostupnosti sistema za zakazivanje i vođenje medicinske dokumentacije, kao i kompromitovanje poverljivosti osetljivih zdravstvenih podataka pacijenata. Ovo bi direktno ometalo sposobnost ordinacije da pruža zdravstvene usluge. S obzirom na nizak nivo rizika, verovatnoća ovakvog scenarija je trenutno ograničena, ali potencijalni uticaj na osetljive podatke iz zdravstvenog sektora ostaje značajan ukoliko se dogodi.

Pregled nivoa rizika po oblastima

Tematska oblast	Nivo rizika
Upravljanje i organizaciona struktura	veoma visok
Politike bezbednosti i klasifikacija	veoma visok
Upravljanje pristupom i identitetima	veoma visok
Prihvatljivo korišćenje i svest zaposlenih	visok
Tehnička zaštita mreže i sistema	visok

Upravljanje podacima i skladištenjem	visok
Monitoring i evidencije	visok
Cloud servisi i spoljni IT provajderi	veoma visok
Reagovanje na incidente i oporavak	visok
Fizička bezbednost	visok
Odnos sa trećim stranama	nema podataka
Licenciranje softvera i legalnost sistema	nizak

Zaključak

Sveobuhvatna analiza rizika informacione bezbednosti u [NAZIV FIRME] ukazuje na ozbiljnu i sistemsku izloženost riziku, koja zahteva hitnu reakciju rukovodstva. Najkritičniji nalazi odnose se na oblasti upravljanja i organizacione strukture, politika bezbednosti i klasifikacije podataka, upravljanja pristupom i identitetima, kao i cloud servisa i spoljnih IT provajdera, koje su ocenjene veoma visokim nivoom rizika. Ovo su temeljne oblasti na kojima počiva čitav sistem zaštite — njihova slabost znači da ordinacija trenutno nema jasno definisan okvir odgovornosti, pravila i kontrolnih mehanizama, što posebno zabrinjava s obzirom na to da se obrađuju osetljivi zdravstveni podaci pacijenata i da ključni poslovni proces, vođenje medicinske dokumentacije i zakazivanje, u potpunosti zavisi od IKT sistema. Konsolidacija svih nadležnosti kod jednog lica, [IME ODGOVORNOG LICA], dodatno naglašava potrebu za formalizacijom i raspodelom odgovornosti, jer se trenutni model oslanja isključivo na jednu osobu bez institucionalne redundanse.

Pored navedenih, visok nivo rizika zabeležen je i u oblastima prihvatljivog korišćenja i svesti zaposlenih, tehničke zaštite mreže i sistema, upravljanja podacima i skladištenjem, monitoringa i evidencija, reagovanja na incidente i oporavka, kao i fizičke bezbednosti. Ove oblasti predstavljaju operativni sloj zaštite i njihova trenutna ranjivost, u kombinaciji sa nedostatkom čvrstog upravljačkog okvira, značajno povećava verovatnoću da bi bezbednosni incident — poput neovlašćenog pristupa, gubitka podataka ili prekida rada sistema — doveo do direktnog ugrožavanja pružanja zdravstvenih usluga i narušavanja poverljivosti podataka pacijenata, sa mogućim pravnim i reputacionim posledicama. Jedina oblast sa niskim rizikom jeste licenciranje softvera i legalnost sistema, što predstavlja pozitivan nalaz i pokazuje da ordinacija vodi računa o formalnoj usklađenosti u ovom segmentu, te da postoji osnova za dalje unapređenje po uzoru na ovu dobru praksu.

Prioritet delovanja treba usmeriti na uspostavljanje osnovnog upravljačkog i organizacionog okvira informacione bezbednosti — jasno definisanje politika, klasifikacije podataka i kontrola pristupa, kao i formalizaciju odnosa sa spoljnim IT provajderima i cloud servisima. Ove oblasti predstavljaju koren većine identifikovanih rizika i njihovo rešavanje će imati najveći uticaj na smanjenje ukupne izloženosti, jer stvaraju preduslove za unapređenje svih ostalih, operativnih oblasti zaštite.

Imajući u vidu prirodu delatnosti i osetljivost podataka sa kojima [NAZIV FIRME] radi, preporučuje se da rukovodstvo u narednom periodu izradi akcioni plan sa jasno

definisanim prioritetima, rokovima i nosiocima aktivnosti, počev od oblasti sa veoma visokim rizikom. Preporučuje se i razmatranje angažovanja spoljne stručne podrške za uspostavljanje politika i kontrola, s obzirom na to da trenutni kapacitet oslonjen na jedno lice nije dovoljan za sveobuhvatno upravljanje bezbednošću. Redovno praćenje sprovođenja mera i periodično ponavljanje analize rizika treba da postanu sastavni deo poslovne prakse, kako bi se obezbedila kontinuirana zaštita poverljivosti, integriteta i dostupnosti podataka pacijenata.

Analizu uradio: Biro za digitalnu bezbednost d.o.o.

Datum izrade: 07.11.2026.

Rukovodstvo Dr Tijana potvrđuje da je upoznato sa sadržajem ove analize rizika.

U _____, ____.____._____. godine

M.P.

Ovlašćeno lice:

_____

Prilozi

Prilog 1: Registar resursa

Kategorija	Tip	Naziv	Vlasnik	Kritičnost
Hardver	Serveri	Lokalni fajl/aplikativni server	Spoljni IT saradnik	kritična
Hardver	Radne stanice / računari	Radne stanice (recepcija, ambulante, administracija)	IT saradnik / zaposleni	visoka
Hardver	Mrežna oprema (ruteri, svičevi)	Ruteri i svičevi na obe lokacije	Spoljni IT saradnik	srednja
Hardver	Mobilni uređaji	Službeni mobilni telefoni/tableti lekara	Zaposleni lekari	srednja
Hardver	Štampači / skeneri / MFP	Mrežni štampači/skeneri	Administracija	niska

	uređaji			
Informacije	Zdravstveni podaci	Medicinski kartoni i nalazi pacijenata	Dr Tijana Jovanović	kritična
Informacije	Podaci o ličnosti klijenata	Lični i kontakt podaci pacijenata	Administracija	visoka
Informacije	Podaci o ličnosti zaposlenih	Kadrovski podaci zaposlenih	Administracija	visoka
Informacije	Finansijski podaci	Finansijski i računovodstveni podaci	Spoljna knjigovodstvena agencija	srednja
Lokacije	Glavna kancelarija	Glavna ordinacija - Beograd, Vračar	Dr Tijana Jovanović	kritična
Lokacije	Poslovna jedinica / filijala	Filijala - Novi Beograd	Vođa filijale	visoka
Lokacije	Serverska soba / data centar	Serverska soba (glavna lokacija)	Spoljni IT saradnik	kritična
Softver	Sistem za upravljanje dokumentima	Sistem elektronskog kartona pacijenata	Dr Tijana Jovanović	kritična
Softver	Sistem za e-poštu	Poslovna e-pošta (cloud)	Administracija	visoka
Softver	Računovodstveni softver	Računovodstveni softver	Spoljna knjigovodstvena agencija	srednja
Softver	Veb sajt / portal	Veb sajt za online zakazivanje	Spoljni dobavljač	srednja
Softver	Alati veštačke inteligencije	AI alat za transkripciju nalaza (u razmatranju)	Dr Tijana Jovanović	niska
Treće strane	IT / cloud provajder	Spoljni IT saradnik i hosting provajder	-	visoka
Treće strane	Pružalac usluga sa pristupom podacima	Eksterna laboratorija za analize	-	visoka
Treće strane	Dobavljač opreme / softvera	Dobavljač softvera za elektronski karton	-	kritična
Treće strane	Podizvođač	Spoljna knjigovodstvena agencija	-	srednja
Zaposleni	Rukovodstvo / menadžment	Direktor ordinacije	-	kritična
Zaposleni	Zaposleni sa pristupom osetljivim podacima	Lekari i medicinske sestre	-	visoka
Zaposleni	Opšti korisnici	Administrativno/recepcijsko osoblje	-	srednja
Zaposleni	Spoljni saradnici / konsultanti	Spoljni IT saradnik	-	visoka

Prilog 2: Registar rizika (pojedinačne pretnje)

Šifra	Pretnja	Odgovor	Verovatnoća	Uticaj	Rizik	Nivo
§3.1	Da li zaposleni imaju pisana uputstva za rad sa ključnim sistemima?	nedefinisano	5	4	20	veoma visok
§3.16	Da li se pristup podacima dodeljuje samo onima kojima je zaista potreban?	nedefinisano	5	4	20	veoma visok
§3.9	Postoje li pravila o tome kako se osetljivi podaci smeju deliti (imejl, štampa)?	nedefinisano	5	4	20	veoma visok
§4.10/4.12	Postoji li kontrola koja sprečava neovlašćenu izmenu ili otkrivanje ključnih podataka?	nedefinisano	5	4	20	veoma visok
§4.3	Koristite li višefaktorsku autentikaciju (MFA) za pristup ključnim sistemima?	nedefinisano	5	4	20	veoma visok
§5.5/5.8	Je li ugovorom definisano postupanje po zahtevu državnih organa i podrška u slučaju incidenta?	nedefinisano	5	4	20	veoma visok
§5.7	Je li sa provajderom potpisan ugovor koji reguliše obradu ličnih podataka?	nedefinisano	5	4	20	veoma visok
§6.1	Postoji li procedura za hitno oduzimanje pristupa zaposlenom koji napušta firmu ili menja poziciju?	nedefinisano	5	4	20	veoma visok

§1.4	Da li postoji plan oporavka u slučaju velike prirodne nepogode (zemljotres, poplava)?	ne	4	4	16	visok
§2.8	Da li ste razmotrili rizik da sadašnja enkripcija bude probijena budućim (kvantnim) računarstvom?	ne	4	4	16	visok
§3.14	Postoji li zamena za ključne IT uloge u slučaju odsustva?	ne	4	4	16	visok
§3.15	Prolaze li zaposleni obuku iz informacione bezbednosti?	ne	4	4	16	visok
§3.17	Postoji li osoba ili tim formalno zadužen za informacionu bezbednost?	ne	4	4	16	visok
§3.18/3.19	Imate li način da primetite neuobičajenu aktivnost, i plan za slučaj prestanka rada ključnog sistema?	ne	4	4	16	visok
§3.2	Da li postoji provera „drugog para očiju“ za kritične IT izmene?	ne	4	4	16	visok
§3.20/3.21	Jesu li osetljivi podaci enkriptovani, i da li testirate uspešnost obnavljanja rezervnih kopija?	ne	4	4	16	visok
§3.23	Da li se podaci nepovratno brišu po isteku propisanog ili ugovorenog roka čuvanja?	ne	4	4	16	visok

§4.11	Jesu li rezervne kopije zaštićene od brisanja čak i sa kompromitovanog naloga (offline/odvojene)?	ne	4	4	16	visok
§4.14/4.16/4.17	Jesu li prostorije sa opremom fizički obezbeđene (brave, alarm, video nadzor)?	ne	4	4	16	visok
§4.18	Imate li mere specifično usmerene protiv ransomver napada (nepromenljive kopije, segmentacija mreže)?	ne	4	4	16	visok
§4.19	Jesu li zaposleni obučeni da prepoznaju socijalni inženjering (lažni pozivi, fišing)?	ne	4	4	16	visok
§4.21	Je li rad na daljinu zaštićen (VPN ili ekvivalentna bezbedna veza, enkriptovana komunikacija, mere protiv neovlašćenog pristupa sa udaljenih/mobilnih uređaja)?	ne	4	4	16	visok
§4.4	Proverava li se periodično ko ima koja prava pristupa, uz uklanjanje nepotrebnih?	ne	4	4	16	visok
§5.9/5.10	Jesu li zaposleni upoznati sa rizikom AI-generisanih prevara, i jesu li podaci uneti u AI	ne	4	4	16	visok

	alate zaštićeni?					
§2.4	Da li imate rezervnu opremu ili plan za slučaj kvara ključnog hardvera/softvera?	nedefinisano	5	3	15	visok
§3.11	Da li se izmene prvo testiraju pre primene na produkcionom sistemu?	nedefinisano	5	3	15	visok
§3.4	Da li se podešavanja sistema proveravaju pre puštanja u rad?	nedefinisano	5	3	15	visok
§4.20	Jesu li mrežni štampači/skeneri ažurirani i zaštićeni lozinkom?	nedefinisano	5	3	15	visok
§4.5	Postoji li politika o dozvoljenom korišćenju IT opreme i interneta?	nedefinisano	5	3	15	visok
§3.12	Da li se prati iskorišćenost kapaciteta sistema (prostor, memorija)?	ne	4	3	12	srednji
§3.3	Da li se evidencije (logovi) o aktivnostima redovno čuvaju i proveravaju?	ne	4	3	12	srednji
§4.1	Jesu li evidencije aktivnosti zaštićene od izmene/brisanja od strane neovlašćenih lica?	ne	4	3	12	srednji
§1.1	Da li imate sistem za detekciju i gašenje požara u prostorijama sa opremom?	da	2	4	8	nizak
§1.2	Da li su te	da	2	4	8	nizak

	prostorije zaštićene od prodora vode (poplava, curenje cevi)?					
§1.3	Da li su prostorije klimatizovane i zaštićene od prekomerne vlage/prašine?	da	2	4	8	nizak
§2.1	Da li se temperatura i vlažnost u serverskoj prostoriji redovno nadgledaju?	da	2	4	8	nizak
§2.2	Da li imate rezervno napajanje (UPS, agregat) za ključnu opremu?	da	2	4	8	nizak
§2.9	Da li su USB portovi i prenosivi medijumi kontrolisani ili skenirani pre upotrebe?	da	2	4	8	nizak
§3.13	Postoji li procedura za prijavu gubitka ili krađe opreme?	da	2	4	8	nizak
§3.5	Je li jasno definisano ko je odgovoran za svaki sistem i proces?	da	2	4	8	nizak
§3.7	Postoji li kontrola verzija ili potvrda pre trajnih izmena važnih podataka?	da	2	4	8	nizak
§3.8	Da li redovno pravite rezervne kopije podataka?	da	2	4	8	nizak
§4.7	Jesu li lozinke lične, uz zabranu deljenja naloga?	da	2	4	8	nizak
§2.3	Je li oprema zaštićena od elektromagnetnih	da	2	3	6	nizak

	smetnji (uzemljenje, razmak od izvora)?					
§2.5	Da li imate rezervnu internet/telekom vezu ako primarna otkaže?	da	2	3	6	nizak
§3.10	Da li redovno ažurirate softver i operativne sisteme?	da	2	3	6	nizak
§3.6/4.6	Da li imate zaštitu od zlonamernog softvera (antivirus i sl.) na svim uređajima?	da	2	3	6	nizak
§4.13	Preuzima li se softver isključivo iz pouzdanih, zvaničnih izvora?	da	2	3	6	nizak
§4.2	Je li pristup podešavanjima sistema ograničen samo na ovlašćene administratore?	da	2	3	6	nizak

Prilog 3: GAP analiza — usklađenost sa članom 10 Zakona

#	Mera (čl. 10 st. 4)	Status	Dokaz (šifre pretnji)
1	Organizaciona struktura	nije ispunjeno	§3.5, §3.17
2	Prikupljanje podataka o pretnjama	nije ispunjeno	§usk_5, §tech_17
3	Bezbednost rada na daljinu	nije ispunjeno	§4.21
4	Osposobljenost lica koja koriste sistem	nije ispunjeno	§3.15, §4.19, §5.9/5.10
5	Dovoljno resursa	nije ispunjeno	§usk_8
6	Zaštita pri promeni poslova zaposlenih	nejasno	§6.1
7	Identifikovanje informacionih dobara	ispunjeno	§registar-resursa
8	Klasifikacija podataka	nije ispunjeno	§org_5
9	Zaštita nosača podataka	ispunjeno	§2.9

10	Ograničenje pristupa	nije ispunjeno	§3.16, §4.4, §4.10/4.12
11	Odobravanje ovlašćenog pristupa	ispunjeno	§4.2
12	Odgovornost korisnika	nejasno	§4.5, §4.7
13	Kriptografske kontrole	nije ispunjeno	§2.8, §3.20/3.21
14	Zaštita od oticanja podataka	nije ispunjeno	§3.9, §4.10/4.12, §5.9/5.10
15	Fizička zaštita objekata	nije ispunjeno	§1.1, §1.2, §1.3, §2.1, §2.3, §4.14/4.16/4.17
16	Zaštita od gubitka	nije ispunjeno	§2.2, §3.13, §3.20/3.21, §4.11, §4.18
17	Ispravnost sredstava	nejasno	§2.7
18	Procedure za računarstvo u klaudu	nejasno	§5.1, §5.2, §5.3, §5.6
19	Praćenje sistema	nije ispunjeno	§3.12, §3.18/3.19
20	Ograničenje pristupa veb prezentacijama	nije ispunjeno	§tech_15
21	Zaštita od zlonamernog softvera	ispunjeno	§3.6/4.6
22	Rezervne kopije podataka	ispunjeno	§3.8
23	Čuvanje podataka o događajima	nije ispunjeno	§3.3, §4.1
24	Integritet softvera	ispunjeno	§3.7, §4.13
25	Zaštita od zloupotrebe slabosti	nejasno	§3.10, §4.20
26	Zaštita pri revizorskom testiranju	nije ispunjeno	§tech_12
27	Zaštita podataka u mrežama	nejasno	§4.8/4.9
28	Bezbednost podataka u komunikaciji	nejasno	§4.8/4.9
29	Zahtevi tokom životnog ciklusa	nije ispunjeno	§3.2, §3.4, §3.11
30	Zaštita test podataka	nejasno	§3.22
31	Procedure čuvanja i brisanja	nije ispunjeno	§3.23, §5.4

32	Zaštita sredstava dostupnih pružaocima	nejasno	§5.5/5.8, §5.7
33	Održavanje ugovorenog nivoa usluge	nejasno	§5.1
34	Prevencija incidenata	nije ispunjeno	§4.15, §4.18, §5.5/5.8
35	Kontinuitet poslova	nije ispunjeno	§1.4, §2.4, §2.5, §3.14, §3.18/3.19
36	Usvajanje dokumenata	nejasno	§3.1
37	Multifaktorska autentifikacija	nejasno	§4.3

Za proveru (odgovor „Ne znam“)

§2.7 — Da li se redovno proverava ispravnost medijuma za skladištenje podataka?

§3.22 — Da li se za testiranje IKT sistema koriste podaci bez stvarnih ličnih/osetljivih podataka (ili se takvi test podaci posebno zaštite)?

§4.15 — Je li vaš sajt/onlajn usluga zaštićena od preopterećenja velikim brojem zahteva (DoS)?

§4.8/4.9 — Je li mrežni saobraćaj i komunikacija (VPN, prenos fajlova) zaštićena enkripcijom?

§5.1 — Biste li mogli da promenite cloud provajdera bez velikog poremećaja poslovanja?

§5.2 — Znate li jasno koje bezbednosne obaveze snosi vaša firma, a koje provajder?

§5.3 — Ima li vaš cloud provajder nezavisan bezbednosni sertifikat (npr. ISO 27001)?

§5.4 — Znate li kako provajder trajno briše podatke po raskidu ugovora?

§5.6 — Znate li u kojoj se zemlji fizički nalaze vaši podaci kod cloud provajdera?