UDK 368.03:004.7
DOI: 10.5937/TokOsig2501069T

Dr Iva Tošić[1*]

POSLOVANJE OSIGURAVAJUĆIH DRUŠTAVA U DIGITALNOM OKRUŽENJU – ŠTA NAM DONOSI DORA?

PREGLEDNI RAD

Sažetak

Poslovanje osiguravajućih društava u digitalnom okruženju omogućava niz prednosti poput ubrzanja prometa, lakše dostupnosti usluga osiguranja i smanjenja troškova. Međutim, taj vid poslovanja, osim pomenutih prednosti, sa sobom nosi i brojne rizike, kao što su IKT (informaciono-komunikacione tehnologije) rizici i sajber napadi. Kako bi se prevazišle razlike u regulisanju upravljanja ovim rizicima među državama članicama EU, doneta je Uredba o digitalnoj operativnoj otpornosti (DORA).

U radu autorka nastoji da ukaže na izazove poslovanja osiguravajućih društava u digitalnom okruženju, trenutnu regulativu u pogledu upravljanja IKT rizicima, kao i izazove sa kojima će se države i osiguravajuća društva susresti prilikom primene odredaba DORA-e. Treba imati u vidu da se na taj način unapređuje zaštita korisnika usluga osiguranja, što je glavni cilj regulative EU u poslovanju osiguravajućih društava (Solventnost II).

Ključne reči: DORA, digitalno okruženje, digitalna operativna efikasnost, IKT rizik, sajber incidenti.

I Uvod

Istorijski gledano, finansijski sektor je bio veoma proaktivan u korišćenju informacionih tehnologija za uspostavljanje novih poslovnih modela i optimizaciju

[1] Docent, Pravni fakultet Univerziteta Union, imejl: iva_tosic@hotmail.com; iva.tosic@pravnifakultet.edu.rs. 0000-0002-9786-0757
Rad primljen: 20.12.2024.
Rad prihvaćen: 21.1.2025.

unutrašnjih procesa. Proces digitalne transformacije znatno se ubrzao poslednjih godina i postao je ključan za opstanak društava koja posluju na finansijskom tržištu iz više razloga. Najpre, očekivanja korisnika usluga postala su takva da se sve više ceni dostupnost fleksibilnih usluga koje su prilagođene ličnim potrebama i odmah dostupne bilo gde i u bilo koje vreme. Pored toga, ekonomsko okruženje uticalo je na finansijske institucije da prilagode svoje poslovne modele, lansiraju nove usluge u potrazi za alternativnim izvorima prihoda i poboljšanjem efikasnosti unutrašnjih procesa, kako bi smanjile troškove. Na taj način omogućava se umnožavanje kapaciteta sistema, a troškovi se smanjuju.

Kao rezultat te transformacije, osiguravajuća društva, budući da su deo finansijskog sektora, postaju potpuno zavisna od svoje tehnologije, koja više nije samo instrument za lakše i brže poslovanje, već i diferencijalni i konkurentski faktor. S druge strane, osim brojnih prednosti, visok stepen digitalizacije povećava rizik od sajber incidenata. Dodatno i drugi faktori doprinose tom rastućem riziku, poput složenosti tehnološkog okruženja većine finansijskih institucija, koje im otežava da održavaju adekvatno kontrolno okruženje i čini ih ranjivijim.

Važno je napomenuti sledeće: kako bi sprovela te procese digitalne transformacije i imala pristup tehnološkim inovacijama koje najbolje mogu doprineti njihovom poslovanju, osiguravajuća društva dopunjuju svoje kapacitete pribavljanjem eksternih usluga i kupovinom proizvoda trećih strana. Zato je otpornost i sajber bezbednost tih trećih strana, pogotovo provajdera, postala značajna koliko i otpornost samih društava, jer incidenti koji ih pogađaju mogu uticati na ceo sektor.[2]

Iako neka istraživanja govore da je finansijski sektor jedan od sektora koji je najbolje opremljen za prevazilaženje sajber i IKT rizika, delimično zbog visokog nivoa regulacije i nadzora, otpornost na pomenute rizike među učesnicima u ovom sektoru je neujednačena. Finansijski sektor je bio glavna meta internet napada, usled čega su regulatori i nadzorni organi prepoznali potrebu za ublažavanjem i upravljanjem IKT rizicima i rade na poboljšanju otpornosti i stabilnosti celokupnog finansijskog sistema.[3] Međutim, mere bezbednosti i kontrole koje su primenjene u kompanijama, pogotovo manjim, neretko su nedovoljne za upravljanje novim sajber i IKT rizicima, čija je ekspanzija nastala tokom pandemije virusa kovid 19. U tom periodu ubrzan je proces automatizacije i digitalizacije na tržištu osiguranja.[4] Zbog toga nije iznenađujuće što su se među institucijama koje su zabeležile najveći porast broja sajber napada, između ostalih, naročito izdvojila i osiguravajuća društva (koja pripadaju

[2] Silvia Senabre, Iván Soto, José Munera, „Strengthening the Cyber Resilience of the Financial Sector - Developments and Trends", *Financial Stability Review*, 2021, 89-90.

[3] Philipp S. Krüger, Jan-Philipp Brauchle, *The European Union, Cybersecurity, and the Financial Sector: A Primer*, Cyber Policy Initiative Working Paper Series – „Cybersecurity and the Financial System", Carnegie Endowment for International Peace , Washington, 2021, 6.

[4] Jelena Ž. Kočović *et al.*, „Pravci razvoja tržišta osiguranja", *Tokovi osiguranja*, 3/2024, 540.

sektoru gde je koncentrisan veliki broj malih institucija).[5] Specifična priroda sajber pretnji koje su obično prekogranične i nisu ograničene na pojedinačne jurisdikcije, dovodi do internacionalizacije kako napada tako i odgovora i njihovog međunarodnog uticaja (direktnog i indirektnog uticaja kroz „efekat zaraze"). Evropska unija, u tom smislu, postaje sve aktivnija u donošenju pravne regulative u tom pogledu, radi stvaranja digitalne operativne efikasnosti kompanija.[6] Među najznačajnijim izdvaja se Direktiva NIS 2,[7] a zatim i Uredba o digitalnoj operativnoj efikasnosti (DORA),[8] koja predstavlja *lex specialis* i koju će od 2025. godine morati da implementiraju društva koja posluju u finansijskom sektoru.

II Pojam digitalne operativne efikasnosti

Digitalna operativna efikasnost predstavlja sposobnost društva da izgradi, održi i preispituje svoju operativnu celovitost i pouzdanost, tako da upotrebom IKT usluga obezbedi sigurnost mrežnih i informacionih sistema kojima se služi i putem kojih se omogućava kontinuirano pružanje finansijskih usluga i njihov kvalitet. Važnost digitalne otpornosti je prirodan rezultat napretka digitalizacije i dva povezana izazova, sajber i IKT rizika.[9] Predložena regulativa EU zahtevaće od osiguravajućih društava da uspostave interne okvire upravljanja i kontrole sposobne da obezbede efikasno i mudro upravljanje IKT rizicima. Iako će ta obaveza biti delegirana posebnoj funkciji u okviru osiguravajućeg društva, uprava će biti odgovorna za sve propuste, imajući u vidu njenu obavezu da odobri i nadgleda upravljanje ovim rizicima.[10] DORA ima za cilj da uvede harmonizovan i sveobuhvatan okvir za digitalnu operativnu otpornost evropskih finansijskih institucija, jasno navodeći eksplicitne zahteve za rešavanje i ublažavanje IKT i sajber rizika. To je direktan odgovor na zajednički savet Evropskih nadzornih agencija (European Supervisory Authorities – ESA). ESA su

[5] S. Senabre, I. Soto, J. Munera, 90.

[6] Paweł Pelc, „The Role of Cybersecurity in the Public Sphere – The European Dimension. Financial Institutions", in: *The Role of Cybersecurity in the Public Sphere – The European Dimension* (eds. K. C. Jentkiewicz, I. Hoffman), Maribor, 2022, 60.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, *Official Journal of the European Union L333/80* - NIS 2 Directive.

[8] Regulation (EU) 2022/2554 of the European Parliament And of The Council Of 14 December 2022 on Digital Operational Resilience For The Financial Sector And Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, *Official Journal of the European Union L333/1* – DORA.

[9] Jose Ramon Martínez Resano, „Digital Resilience and Financial Stability - The Quest For Policy Tools in The Financial Sector", *Revista de Estabilidad Financiera*, 2022, 65.

[10] Pierpaolo Marano, Michele Siri, „Regulating Insurtech in The European Union", *Journal of Financial Transformation,* 2021, 173.

identifikovale četiri oblasti delovanja na koje se treba usredsrediti u regulatornom razvoju u bliskoj budućnosti: prvo, zahtevi za IKT bezbednost i upravljanje rizicima; drugo, sektorski zahtevi za izveštavanje o sajber incidentima; treće, direktni nadzor i supervizija pružalaca usluga trećih strana; i četvrto, okvir za testiranje sajber otpornosti. DORA reguliše sva ta pitanja i pruža potencijalne odgovore i rešenja za trenutne pravne praznine.[11]

III Poslovanje osiguravajućih društava u digitalnom okruženju

Tehnološki napredak i razvoj digitalnih tehnologija omogućava osiguravajućim društvima da poboljšaju svoje poslovanje, ali i da unaprede korisničko iskustvo. Digitalizacija omogućava najpre analizu velike količine podataka koja postaje ključna za donošenje informisanih odluka u delatnosti osiguranja. Na taj način, analizom istorijskih podataka, osiguravajuća društva mogu preciznije proceniti rizike i prilagoditi polise, čime se omogućava personalizacija ponude korisnicima. Na osnovu podataka o ponašanju korisnika, moguće je kreirati prilagođene polise osiguranja koje se zasnivaju na potrebama konkretnog korisnika. Sledeća značajna prednost je optimizacija procesa obrade šteta, jer se automatizacijom analize podataka ubrzavaju procesi obrade šteta i na taj način smanjuje vreme potrebno za rešavanje zahteva. Osim navedenog, korišćenje veštačke inteligencije i digitalnih platformi omogućava automatsku obradu zahteva smanjujući potrebu za ljudskom intervencijom. Algoritmi veštačke inteligencije mogu analizirati obrasce ponašanja i identifikovati sumnjive aktivnosti, smanjujući rizik od prevara. I kao najvažnije, imajući u vidu da je poverenje korisnika usluga osiguranja stavljeno u centar svih aktivnosti osiguravajućih društava, na taj način omogućava se poboljšanje podrške korisnicima usluga. Međutim, kao što donosi mnoge prednosti, digitalizacija takođe stavlja osiguravajuća društva pred velike izazove. Imajući u vidu da obrađuju velike količine osetljivih podataka, uključujući lične i finansijske podatke svojih korisnika, zaštita ovih podataka od sajber napada postaje ključni prioritet. Primeri incidenata pokazuju koliko su osiguravajuća društva ranjiva na sajber pretnje, što može dovesti do gubitka poverenja korisnika i značajnih finansijskih gubitaka. Stoga, danas upravljanje IKT rizicima i sajber bezbednost predstavljaju jednu od značajnih obaveza i ciljeva u poslovanju. Tokom procesa prilagođavanja promenama u poslovanju zahtevaće se usaglašavanje s brojnom i često promenljivom regulativom, ulaganje u modernu IT infrastrukturu i njeno održavanje, kontinuirano investiranje u nadogradnju sistema i obuku zaposlenih. Prilagođavanje digitalnoj transformaciji zahteva promenu poslovne kulture, a uspostavljanje inovativnog i fleksibilnog radnog okruženja ključno je za uspeh digitalne transformacije.

[11] P. S. Krüger, J.P. Brauchle, 4.

IV Upravljanje IKT rizicima u osiguravajućim društvima

Brzina kojom se IT okruženje menja i razvija svakodnevno izlaže tržište osiguranja i njegovo okruženje novim rizicima. Pravovremene mere kontrole rizika moraju se kontinuirano evaluirati kako bi se osiguralo da budu i dalje efikasne u identifikaciji i upravljanju rizicima s kojima se ova društva susreću.[12] Direktiva Solventnost II[13] stupila je na snagu 2016. godine kako bi harmonizovala regulativu osiguranja u EU. Međutim, ona ne reguliše eksplicitno IKT rizike i sajber bezbednost, već ih implicitno obrađuje kao deo operativnih rizika. Član 41 Direktive Solventnost II zahteva od osiguravajućih društava da uspostave efikasan sistem upravljanja koji omogućava upravljanje poslovima pažnjom dobrog stručnjaka. Ta društva treba da preduzmu razumne korake kako bi osigurala kontinuitet u obavljanju svojih aktivnosti, uključujući razvoj planova za vanredne situacije. Društva za osiguranje „moraju primeniti odgovarajuće i proporcionalne sisteme, resurse i procedure". U skladu sa članom 44, kao deo sistema upravljanja, moraju „imati uspostavljen efikasan sistem za upravljanje rizicima... kako bi identifikovale, merile, nadzirale, upravljale i izveštavale, na kontinuiranoj osnovi, o rizicima, pojedinačno i na agregiranom nivou, kojima su izložene ili bi mogle biti izložene, kao i o njihovim međuzavisnostima". Na taj način Direktiva uređuje upravljanje svim rizicima kojima je društvo izloženo, bez eksplicitne analize IKT rizika. S obzirom da evropska regulativa koja se odnosi na osiguravajuća društva ne obrađuje specifično pravilno upravljanje IKT i sajber rizicima, regulativa zemalja članica često se znatno razlikuje. Dok neke zemlje, kao što je npr. Nemačka, imaju specifične zahteve za IKT sigurnost i upravljanje u sektoru osiguranja,[14] druge zemlje nemaju nikakvu regulativu u pogledu ovog pitanja. To pokazuje snažnu potrebu za harmonizacijom evropske regulative u pogledu pitanja upravljanja i prevazilaženja ovih rizika.[15]

Evropska nadzorna tela (ESA), kao što smo pomenuli, zaključuju da trenutni fragmentiran regulatorni i nadzorni pejzaž može dovesti do nekonzistentnih praksi širom Evrope i ugroziti ravnopravno poslovanje. Stoga je predlog da se u odgovarajućim podsektorima utvrde opšti zahtevi za upravljanje IKT rizicima i omogući sajber bezbednost, kako bi se stvorili uslovi za sigurno pružanje usluga. Takva harmonizacija pomogla bi u promovisanju veće IKT sigurnosti i sajber bezbednosti. U skladu s tim Evropsko nadzorno telo za osiguranje i penzijske fondove (EIOPA) objavilo je Smernice

[12] Simon Grima, Pierpaolo Marano, „Designing a Model for Testing the Effectiveness of a Regulation: The Case of DORA for Insurance Undertakings", *Risks*, 9/2021, 2.

[13] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), *Official Journal of the European Union L335/1* - Solventnost II.

[14] Federal Financial Supervisory Authority (Bafin), „Supervisory Requirements for IT in Insurance Undertakings", 2022.

[15] P. S. Krüger, J.P. Brauchle, 16-17.

o sigurnosti i upravljanju na području informacionih i komunikacionih tehnologija (EIOPA Smernice).[16] EIOPA Smernice pokrivaju oblasti upravljanja IKT rizicima, strategiju IKT-a, politiku i mere informacione sigurnosti, sigurnost IKT operacija i upravljanje IKT operacijama, upravljanje promenama IKT-a, planove odgovora i oporavka itd. One su izrađene na osnovu Smernica Evropskog bankarskog nadzornog tela (EBA)[17] kako bi se osigurala doslednost među podsektorima. Te smernice predviđaju obavezu uprave društva da omogući da se pomoću sistema upravljanja odnosno funkcije upravljanja rizicima i sistema internih kontrola na odgovarajući način upravlja IKT i sigurnosnim rizicima. Osim toga, društvo mora voditi računa da broj članova i njihove veštine (*fit and proper*) budu prikladni za pružanje podrške operativnim potrebama na području IKT-a, postupcima upravljanja rizicima IKT-a i sigurnosnim rizicima na kontinuiranoj osnovi, kako bi se obezbedilo sprovođenje strategije IKT-a.[18] I ovde se primenjuje načelo proporcionalnosti, tačnije pravo društava da EIOPA Smernice primenjuju na način u skladu s prirodom, obimom i složenošću rizika kojima su izložena. Osiguravajuća društva treba da uspostave programe osposobljavanja za informacionu sigurnost za sve zaposlene, uključujući članove uprave, kako bi se obezbedilo da budu osposobljeni za izvršavanje svojih dužnosti i odgovornosti. Osim toga, treba da organizuju i sprovedu periodične programe za podizanje svesti o sigurnosti, o tome kako postupati s rizicima povezanim s informacionom sigurnosti.[19]

V DORA u osiguravajućim društvima

Kao što smo prethodno pomenuli, pandemija izazvana globalnim širenjem kovida 19 i njen efekat na poslovanje društava bili su katalizatori za ubrzanje digitalizacije.[20] Suočavajući se s regulatornom fragmentacijom koja je nastala, EU je odlučila da predstavi DORA-u. DORA je usklađeni pristup EU da zameni ono što se naziva „nekoordinisanim nacionalnim inicijativama".[21] Uredba postavlja jedinstvene zahteve u vezi sa bezbednošću mrežnih i informacionih sistema koji podržavaju poslovne procese finansijskih entiteta, neophodne za postizanje visokog zajedničkog

[16] European Insurance and Occupational Pensions Authority (EIOPA), Smernice o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija, EIOPA-BoS-20/600 – EIOPA Smernice.

[17] *Smernice EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima*, EBA/GL/2019/04, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880816/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_HR.pdf, 10.07.2024.

[18] EIOPA Smernice, Smernica 2.

[19] EIOPA Smernice, Smernica 13.

[20] Za više o uticaju pandemje virusa kovid 19 na poslovanje sektora osiguranja u Republici Srbiji v: Marko R. Risimović, Zlata I. Đurić, Nađa M. Đurić, „Poslovanje sektora osiguranja u Republici Srbiji u uslovima pandemije kovida 19", *Tokovi osiguranja*, 1/2022, 111-129.

[21] Stavros Kourmpetis, „Management of ICT Third Party Risk Under the Digital Operational Resilience Act", *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, Palgrave Macmillan, 2023, 220.

nivoa digitalne operativne otpornosti.[22] Predlogom DORA, Evropska komisija je direktno odgovorila na preporuke ESA i prepoznajući rizike koji mogu proizaći iz nedostatka detaljnih i sveobuhvatnih pravila u ovoj oblasti predlaže da DORA ima veoma široku primenu i da pokrije gotovo sve finansijske institucije iz sva tri podsektora.[23] Radi postizanja digitalne operativne otpornosti, predlaže se da društva uspostave i održavaju otporne IKT sisteme i alat koji minimizira uticaj IKT rizika; da kontinuirano identifikuju sve izvore IKT rizika; da uspostave zaštitne, preventivne i detektivne mere; da uspostave posvećene i sveobuhvatne politike za ostvarivanje kontinuiteta poslovanja i planove za vanredne situacije i oporavak kao integralni deo operativne politike kontinuiteta poslovanja. Regulativa sama po sebi ne nameće specifičnu standardizaciju, već se oslanja na evropske i međunarodno priznate tehničke standarde ili najbolje prakse u industriji.

1. Ciljevi i značaj DORA-e

U EU, DORA omogućava harmonizaciju u regulisanju digitalne operativne otpornosti.[24] Glavni cilj je otpornost finansijskog sektora, među ostalim i u operativnom smislu, kako bi se osigurala njegova tehnološka sigurnost i dobro funkcionisanje, brz oporavak od povreda i incidenata na području IKT-a, a time obezbedilo delotvorno i neometano pružanje finansijskih usluga u celoj EU, uz očuvanje poverenja potrošača u tržište.

Na taj način omogućava se konsolidacija i unapređenje zahteva u pogledu IKT rizika koji je do sada bio obuhvaćen operativnim rizikom u različitim pravnim aktima Unije (pa tako i Direktivom Solventnost II u osiguravajućim društvima). Iako su tim aktima obuhvaćene glavne kategorije finansijskih rizika (npr. kreditni rizik, tržišni rizik, rizik likvidnosti, rizik ponašanja na tržištu), njima u vreme donošenja nisu sveobuhvatno obrađene sve komponente operativne otpornosti. Odredbe koje se odnose na operativne rizike često su se zasnivale na tradicionalnom kvantitativnom pristupu upravljanju rizikom, te nisu bila obuhvaćena kvalitativna pravila za zaštitu, otkrivanje, ograničenje, oporavak, izveštavanje i digitalno testiranje u slučaju IKT napada. Konsolidovanjem i ažuriranjem različitih pravila o IKT rizicima, sve odredbe koje se odnose na digitalne rizike u finansijskom sektoru na ovaj način su dosledno objedinjene u jedinstveni zakonodavni akt. Na taj način DORA omogućava popunjavanje pravnih praznina i uklanjanje nedoslednosti u nekim prethodnim pravnim aktima, između ostalog u vezi s terminologijom koja se u njima upotrebljava. Ona izričito definiše IKT rizik, upravljanje IKT rizicima, izveštavanje o incidentima, testiranje

[22] Luís Barroso,„Fintechs: Concept, Level Playing Field and the Supervisory Approach", *Fintech Regulation and the Licensing Principle*, 2023, 43.
[23] P S. Krüger, J. P. Brauchle, 22
[24] J. R. Martínez Resano, 77.

operativne otpornosti i praćenje IKT rizika povezanog s trećim stranama. Na taj način podiže se i svest o IKT rizicima i ukazuje se na činjenicu da IKT incidenti i neadekvatna operativna otpornost mogu ugroziti stabilnost finansijskih subjekata.[25]

Donošenjem jedinstvenog zakonodavnog akta u pogledu digitalne operativne efikasnosti omogućava se da finansijski subjekti slede isti pristup i ista pravila u upravljanju IKT rizicima. Predložene odredbe imaće značajan uticaj na mere sajber bezbednosti koje preduzimaju osiguravajuća društva, takođe kroz uvođenje zahteva za sprovođenje penetracionih testova koji će uticati na njihov rad.[26] Prilikom primene tih pravila, osiguravajuća društva treba da uzmu u obzir veličinu i ukupni profil rizičnosti, te prirodu, opseg i složenost svojih usluga, aktivnosti i poslovanja (načelo proporcionalnosti). Doslednost će doprineti povećanju poverenja u rad osiguravajućih društava, kao i ceo finansijski sektor. Osim toga, omogućava se očuvanje stabilnosti, što je naročito značajno u periodu kada se poslovanje u velikoj meri oslanjanja na sisteme, platforme i infrastrukture IKT-a, što podrazumeva povećani digitalni rizik. Poštovanjem osnovne „digitalne higijene" trebalo bi izbeći nastajanje velikih troškova za privredu, smanjenjem učinka i troškova poremećaja u radu IKT-a na najmanju moguću meru.[27]

2. Uticaj na rad osiguravajućih društava

Osiguravajuća društva, kao i ostatak finansijskog sektora, biće u obavezi da primene te odredbe, što će zahtevati usklađivanje na svim nivoima društva. Osim što je neophodno da na nivou samog društva preduzmu sve mere za prevazilaženje IKT rizika (upravljanje rizikom, izveštavanje o incidentima, testiranje digitalne operativne otpornosti, razmena informacija), naročito značajno je što Uredba uspostavlja i zahteve koji se odnose na ugovorne aranžmane sklopljene s trećim licima koja pružaju IKT usluge, kao i pravila za saradnju između nadležnih tela i nadzor i izveštavanje koji sprovode. U skladu sa odredbama DORA-e, osiguravajuća društva koja nisu mikropreduzeća biće dužna da uspostave nezavisnu kontrolnu funkciju za upravljanje IKT rizicima i obezbede nadzor nad sprovođenjem ove funkcije, koja će biti odvojena od ostalih kontrolnih funkcija i funkcije unutrašnje revizije u skladu s modelom „tri linije odbrane" ili internim modelom upravljanja rizicima i kontrole nad njima.[28] Nezavisnost te kontrolne funkcije je značajna kako bi se izbegli sukobi interesa. Na taj način se jasno ukazuje na to da su, u današnjem digitalnom poslovanju, IKT rizici jedni od primarnih rizika kojima su društva izložena. Sam termin kontrolna funkcija ukazuje na značaj i odgovornost koju neka funkcija nosi. Međutim, bez obzira na

[25] DORA, recital 12.
[26] P. Pelc, 63.
[27] DORA, recital 13.
[28] DORA., čl. 6, st. 4.

obavezu uspostavljanja posebne funkcije za upravljanje IKT rizicima, odgovornost za sve dužnosti u vezi sa upravljanjem njima snosi uprava društva.[29]

Osim navedenog, osiguravajuća društva će, u skladu s principom proporcionalnosti, morati da uspostave funkciju za praćenje ugovornih aranžmana sklopljenih s pružaocima IKT usluga ili da imenuju člana višeg rukovodstva za takav nadzor. Kako bi se redovno evaluirala i pratila sposobnost da usluge pruža bez negativnih učinaka na digitalnu operativnu otpornost osiguravajućeg društva, trebalo bi uskladiti nekoliko ključnih ugovornih elemenata s pružaocima IKT usluga. Takvim usklađivanjem potrebno je da se obuhvate minimalna područja koja su ključna kako bi se društvu omogućilo potpuno praćenje rizika kojima bi moglo biti izloženo od treće strane koja društvu pruža IKT usluge. To je značajno radi očuvanja digitalne otpornosti društva koja je direktno zavisna od stabilnosti, funkcionalnosti, dostupnosti i sigurnosti IKT usluga koje prima.[30]

Potrebno je preduzeti odgovarajuće mere za upravljanje krizama i za sprovođenje strategije za IKT incidente. Od osiguravajućih društava očekuje se implementacija sveobuhvatnog okvira za upravljanje IKT rizicima kao deo celokupnog sistema upravljanja rizicima, uključujući strategije, politike, smernice, procedure, protokole i aplikacije neophodne za sveobuhvatnu i adekvatnu zaštitu svih informacionih i IKT resursa od štetnih uticaja svake vrste.[31] Kako bi bila u mogućnosti da prevaziđu te rizike, društva će morati da uspostave interne procese za otkrivanje, upravljanje i obaveštavanje o incidentima vezanim za IKT,[32] kao i programe za pregled sopstvene digitalne operativne stabilnosti. Na taj način biće u mogućnosti da procene spremnost, identifikuju slabosti, nedostatke ili praznine u digitalnoj operativnoj stabilnosti i implementiraju korektivne mere u ranim fazama.[33] Uredba predviđa punu odgovornost samog društva za pravilno postupanje sa incidentima i posledicama koje usled njega nastanu, bez obzira na pružanje relevantnih povratnih informacija ili opštih smernica od strane nadzornih organa kao meru nakon prijave incidenta.[34] Stoga, osiguravajuća društva biće u obavezi da uspostave mere procene rizika i bezbednosti, kao i da usvoje strategija za upravljanje IKT rizicima kako bi bila u mogućnosti da odgovore na izazove digitalnog okruženja u kome danas posluju.[35]

[29] P. Marano, M. Siri, 173.
[30] DORA, recital 68.
[31] DORA, čl. 6.
[32] DORA, čl. 17.
[33] DORA, čl. 24.
[34] DORA, čl. 22.
[35] Thorsten Ammann, Imran Syed, Vinny Sanchez, „Exploring Operational Resilience in Financial Services – the Effects of DORA on Risk and Regulation in Top 3 Financial Markets", *Computer Law Review International*, 2/2023, 44.

a) Upravljanje IKT rizicima

U savremenom digitalnom okruženju upravljanje IKT rizicima od strane osiguravajućih društava postalo je ključno kako bi društva ostala konkurenta i očuvala poverenje korisnika usluga osiguranja. U skladu sa odredbama Uredbe, upravljanje IKT rizicima sprovodi se kroz nekoliko međusobno povezanih faza: utvrđivanje rizika, zaštitu i sprečavanje, otkrivanje, odgovor i oporavak, učenje i razvoj i komunikaciju.

Da bi se uspešno upravljalo tim rizicima, neophodno je da društvo najpre utvrdi, klasifikuje, dokumentuje i vodi evidencije o svim poslovnim funkcijama koje se oslanjaju i koriste IKT-om. Osim toga, da sprovodi procenu rizika i utvrđuje konkretne izvore IKT rizika, procenjuje eventualne pretnje i ranjivosti i preispituje scenarije rizika. Imajući u vidu da Uredba posebnu pažnju posvećuje rizicima koji dolaze od strane trećih lica koja društvu pružaju IKT usluge, potrebno je utvrditi, dokumentovati i voditi evidencije za sve procese koji zavise od tih lica. U okviru te prve faze neophodno je najmanje jednom godišnje sprovoditi procenu rizika za sve zastarele IKT sisteme.[36]

Kada završe prvu fazu i utvrde rizike, od društava se očekuje da preduzmu sve mere prevencije od IKT rizika. Tokom te faze društvo treba da prati i kontroliše sigurnost i funkcioniranje IKT sistema i uticaj IKT rizika na taj sistem, da uspostavi politiku informacione sigurnosti, razvije pouzdanu strukturu za upravljanje mrežom i infrastrukturom. Takođe, radi sprečavanja nastanka IKT rizika, društva sprovode upravljačke, logičke i fizičke kontrole pristupa IKT imovini, mehanizme autentifikacije, dokumentovane politike, postupke i kontrole za upravljanje promenama IKT-a.[37]

U okviru treće faze koju Uredba naziva „otkrivanje" neophodno je da društvo uspostavi mehanizme za brzo otkrivanje neobičnih aktivnosti, da odredi pragove za upozorenja i kriterijume za aktiviranje i pokretanje procesa odgovora na IKT incidente, što uključuje i mehanizme za automatsko upozoravanje u slučaju izbijanja IKT incidenata.[38] Kada je ova faza završena, potrebno je da društvo bude u mogućnosti da odgovori na IKT incident i oporavi se od njega. Od posebnog značaja će biti obaveza uspostavljanja sveobuhvatne politike kontinuiteta poslovanja na području IKT-a, kao i uvođenje funkcije za upravljanje krizama koju moraju uspostaviti društva koja nisu mikropreduzeća i obaveza da nadzornom telu na zahtev dostave procenu godišnjih troškova i gubitaka koji su prouzrokovani IKT incidentima.[39]

Nakon što IKT incidenti izazovu poremećaje u poslovanju osiguravajućeg društva, važno je da se prikupe sve informacije i izvrši analiza slabostī društva, internet pretnji , IKT incidenata i napada, kao i kakav je njihov uticaj na digitalnu operativnu efikasnost društva. Osiguravajuća društva koja nisu mikropoduzeća na zahtev

[36] DORA, čl. 8.
[37] DORA, čl. 9.
[38] DORA, čl. 10.
[39] DORA, čl. 11.

obaveštavaju nadzorni organ o promenama koje su sprovedene u toku preispitivanja nakon IKT incidenata. Utvrđuje se da li je društvo postupalo u skladu s uspostavljenim postupcima, kao i da li su preduzete mere bile delotvorne. Neophodno je da društvo mapira razvoj IKT rizika, analizira učestalost, vrste, razmere i obrasce incidenata i napada, da sprovede edukaciju i osposobljavanje osoblja putem programa za podizanje svesti o sigurnosti na području IKT-a i digitalnoj operativnoj otpornosti, kao i da prati tehnološka dostignuća kako bi bolje razumelo na koji način ta dostignuća mogu uticati na zahteve u pogledu sigurnosti IKT-a i digitalnu operativnu otpornost.

Kao poslednja faza za upravljanje rizicima javlja se komunikacija koja se ostvaruje izradom planova komunikacije i objavom barem značajnih IKT incidenata ili ranjivosti klijentima, partnerskim finansijskim subjektima i javnosti, zavisno od slučaja. Komunikacione politike se razlikuju u zavisnosti od toga da li se radi o internim politikama ili je u pitanju komunikacija sa spoljnim partnerima, klijentima itd. Iz navedenog vidimo da DORA predviđa jedan sveobuhvatan sistem za upravljanje IKT rizicima, koji od društava zahteva kako uspostavljanje takvog sistema, tako i praćenje i analizu da li su konkretne mere i politike bile delotvorne. Ukoliko se ispostavi suprotno, od društva se očekuje da kontinuirano unapređuje sistem za upravljanje IKT rizicima. Imajući u vidu da se radi o rizicima koji se svakodnevno razvijaju, jedino takav pristup može obezbediti delotvorno upravljanje i prevazilaženje izazova koje digitalno poslovanje donosi osiguravajućim društvima i celom finansijskom sektoru.

b) Upravljanje, klasifikacija i izveštavanje u vezi sa IKT incidentima

DORA propisuje proces upravljanja, klasifikacije IKT incidenata i sajber pretnji, *izveštavanje* o značajnim IKT incidentima i *dobrovoljno obaveštavanje* o ozbiljnim sajber pretnjama.

U okviru procesa upravljanja IKT incidentima, osiguravajuća društva će morati da uspostave proces kojim će evidentirati, pratiti i preduzimati mere za sve IKT incidente i ozbiljne sajber pretnje i dokumentovati njihove uzroke. To obuhvata uspostavljanje sistema za rano upozoravanje, klasifikaciju i kategorisanje IKT incidenata prema ozbiljnosti, zahvaćenosti ključnih usluga, aktivaciju uloga, odgovornosti i planova za unutrašnju i spoljnu komunikaciju, rešavanje prigovora korisnika, izveštavanje višeg rukovodstva barem o značajnim IKT incidentima i uspostavljanje načina odgovora na IKT incidente.[40]

Za klasifikaciju IKT incidenata i sajber pretnji (broj, učinak, trajanje, raširenost, gubitak podataka, ključnost, ekonomski učinak), pripremljen je zajednički nacrt Regulatornih tehničkih standarda (RTS) u kojem su bliže opisani kriterijumi za klasifikaciju IKT incidenata i sajber pretnji, procenu relevantnosti njihovog značaja i ozbiljnosti.[41]

[40] DORA, čl. 17.

[41] Draft Regulatory Technical Standards to Further Harmonise ICT Risk Management Tools, Methods, Processes and Policies as Mandated Under Articles 15 and 16(3) of Regulation (EU) 2022/2554, JC 2023 86, 2024, https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-_Final_report_on_draft_RTS_on_ICT_Risk_Management_Framework_and_on_simplified_ICT_Risk_Management_Framework.pdf, 25. 7. 2024.

Kada je u pitanju izveštavanje o IKT incidentima, DORA pravi razliku između *obaveznog izveštavanja* o značajnim IKT incidentima i *dobrovoljnog obaveštavanja* o ozbiljnim sajber pretnjama, ako društvo smatra da je pretnja relevantna za finansijski sektor. U proces izveštavanja i dobrovoljnog obaveštavanja uključeni su i korisnici usluga koje će osiguravajuće društvo obavezno izveštavati kada je incident takav da utiče na njihove finansijske interese. To je u skladu sa glavnim ciljem koji je postavljen pred osiguravajuća društva, a to je zaštita korisnika usluga osiguranja. Za dugoročno poslovanje tih društava vrlo je značajno da održe dobru poslovnu reputaciju i poverenje korisnika usluga, što je moguće jedino ukoliko ih obaveštavaju o svim pitanjima značajnim za zaštitu njihovih interesa. U slučaju ozbiljne sajber pretnje, važno je da društvo obavesti i klijente, koji bi mogli biti pogođeni, i da ih pouči o odgovarajućim zaštitnim merama čije bi preduzimanje mogli razmotriti.

Izveštavanje koje osiguravajuće društvo sprovodi u odnosu na nadzorni organ se sastoji se od :

- *početnog obaveštenja;*
- *prelaznog izveštaja* (čim se status izvornog incidenta znatno promeni ili se postupanje u vezi sa značajnim IKT incidentom promeni na osnovu novih dostupnih informacija);
- *ažurirana obaveštenja* (prema potrebi, svaki put kad se pojave relevantne novosti o statusu, kao i na izričit zahtev nadzornog organa);
- *završnog izveštaja*.

Nadzorno telo je u obavezi da obavesti EIOPA-u koja procenjuje značaj IKT incidenta i u zavisnosti od sopstvene procene dalje izveštava nadležne regulatore odnosno tela država članica radi preduzimanja mera u cilju očuvanja stabilnosti finansijskog sektora.[42] Za potrebe izveštavanja ESA je izradila zajednički nacrt RTS-ova kojima će detaljnije odrediti sadržaj i rokove izveštavanja i obaveštavanja, kao i standardne šablone, obrasce i postupke za izveštavanje o značajnim IKT incidentima i obaveštavanje o ozbiljnim sajber pretnjama.[43] Osim toga, DORA obavezuje ESA-u da do 17. 1. 2025. izrade zajednički izveštaj u kom će proceniti mogućnost centralizacije izveštavanja o značajnim incidentima kroz uvođenje jedinstvenog centra za izveštavanje o značajnim IKT incidentima.[44]

[42] DORA, čl. 19.

[43] Draft Regulatory Technical Standards on the Content of the Notification and Reports for Major Incidents and Significant Cyber Threats And Determining the Time Limits for Reporting Major Incidents and Draft Implementing Technical Standards on the Standard Forms, Templates and Procedures for Financial Entities to Report a Major Incident and to Notify a Significant Cyber Threat, https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf, 20. 7. 2024.

[44] DORA, čl. 20.

Obaveštenje pruža veću šansu za bolje razumevanje i identifikaciju izvora incidenta, analizu potencijalnih posledica i traženje pomoći. Brzo obaveštavanje o incidentu može takođe pomoći drugim institucijama da se bolje pripreme za slične napade.[45] Na taj način omogućilo bi se brzo reagovanje u slučaju IKT incidenta, na nivou cele EU, i značajno bi se olakšalo upravljanje IKT incidentima, što bi bilo od ogromnog značaja imajući u vidu da su ovakvi incidenti sve češći, kao i da mogu značajno poremetiti funkcionisanje celog finansijskog sektora.

v) Testiranje digitalne operativne otpornosti

U skladu sa odredbama Uredbe, sastavni deo okvira za upravljanje IKT rizicima, incidentima i pretnjama jeste izrada programa testiranja digitalne operativne otpornosti. To obuhvata procenu i skeniranje ranjivosti, mrežne sigurnosti, fizičke sigurnosti, testiranje kompatibilnosti, performansi, integralno testiranje itd. Sprovođenje testiranja može sprovesti nezavisni spoljni ili unutrašnji izvršilac testiranja. Ako se testiranje sprovodi interno, mora se obezbediti nezavisnost, s ciljem izbegavanja sukoba interesa u fazama osmišljavanja i sprovođenja testiranja. Neophodno je da osiguravajuća društva najmanje jednom godišnje sprovedu test IKT sistema i aplikacija kojima se podupiru ključne ili važne funkcije.[46] Osim toga, društva koja nisu mikropreduzeća biće dužna da svake tri godine (učestalost se može smanjiti, ali i povećati u zavisnosti od zahteva nadzornog organa) sprovedu napredna testiranja IKT sistema, alata i procesa na temelju TLPT-a (Threat-Led Penetration Testing).[47] Osiguravajuće društvo mora da proceni koje ključne i važne funkcije će biti obuhvaćene tim testiranjem (funkcije čiji bi poremećaj bitno narušio finansijske rezultate ili sposobnost kontinuiranog ispunjavanja uslova i obaveza društva), a rezultate ove procene potvrđuje nadzorni organ, dok će se sažetak rezultata testiranja dostavljati i određenom jedinstvenom telu javne vlasti koje određuju države članice. Za potrebe sprovođenja naprednog testiranja na osnovu TLPT-a moći će da se angažuju samo odgovarajuća lica unutar ili van društva koja ispunjavaju posebne zahteve i kriterijume koje je propisala DORA, ali i zahteve, standarde i kriterijume povezane s ovim testiranjem koje će izraditi ESA. Na taj način DORA propisuje *fit and proper* uslove koje mora ispunjavati izvršilac koji obavlja testiranje.

[45] Dirk Clausmeier, „Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)", *International Cybersecurity Law Review,* 4/2023, 85.

[46] DORA, čl. 24.

[47] DORA, čl. 26; Ovo testiranje omogućava da se utvrdi kako trenutne pretnje mogu uticati na kritične poslovne funkcije. TLPT je mehanizam za verifikaciju stvarne otpornosti društva koji je ključan za funkcionisanje celog finansijskog sektora.

g) Upravljanje IKT rizikom povezanim s trećim stranama, aranžmani za razmenu informacija i nadzorni organi

DORA poseban fokus stavlja na upravljanje IKT rizikom povezanim s trećim licima, što ne predstavlja potpunu novinu za osiguravajuća društva imajući u vidu da su i do sada imala mogućnost „izdvajanja" (outsourcing) ključnih odnosno važnih poslovnih funkcija. DORA opširno i detaljno reguliše ključna načela dobrog poslovnog upravljanja IKT rizikom povezanog s trećim licima, kao i nadzorni okvir za treća lica koja pružaju IKT usluge. Imajući u vidi da se nove odredbe o digitalnoj operativnoj efikasnosti odnose i na ta lica, ona su barem indirektno pogođena istim regulatornim zahtevima kao i sama osiguravajuća društva. Kao posledica toga, od njih će se zahtevati da ponovo prilagode svoje standardne ugovorne uslove i usluge u skladu sa zahtevima koje postavlja DORA ukoliko žele da zadrže ili čak prošire svoju bazu klijenata.[48]

DORA uređuje razmenu informacija među finansijskim subjektima koje se odnose na sajber pretnje, uključujući pokazatelje ugroženosti, taktike, tehnike i postupke, sigurnosna upozorenja i konfiguracioni alat. Osiguravajuća društva biće u obavezi da obaveštavaju nadzorni organ o učestvovanju u takvim aranžmanima za razmenu informacija.

Uredba navodi spisak nadzornih tela za sve subjekte u finansijskom sektoru i uređuje njihovu međusobnu saradnju, saradnju sa glavnim nadzornim telom i telom osnovanim u skladu sa NIS 2 Direktivom. Takođe, uspostavlja mehanizme za razmenu primera iz prakse koji su se pokazali delotvornim i propisuje ovlašćenja za nadzor, istrage i sankcije potrebne za izvršavanje propisanih zadataka, ovlašćenja izricanja administrativnih kazni i korektivnih mera i objavu administrativnih kazni. Osim navedenog, reguliše dužnost obaveštavanja Komisije, ESMA-e, EBA-e i EIOPA-e o zakonima i propisima kojima se omogućava primena novih odredaba digitalne operativne efikasnosti, čuvanja poslovnih tajni i zaštiti podataka.

Interesantno je da DORA, iako predviđa različite nadzorne i istražne mere, kao i mogućnost izricanja sankcija od stane nadzornog organa kako bi se prisilili adresati novih odredaba da se pridržavaju pravnog i regulatornog okvira, ne pruža eksplicitne novčane kazne ili druge krivične sankcije za nepoštovanje zahteva osim za treća lica koja pružaju IKT usluge.[49] U tom pogledu, regulacija se razlikuje od Opšte uredbe o zaštiti podataka (GDPR)[50] i NIS-2 Direktive.[51] Umesto toga, prema članu 50 DORA-e, članicama EU ostavljeno je da odrede administrativne kazne

[48] T. Ammann, I. Syed, V. Sanchez, 44.

[49] DORA, čl. 35.

[50] 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), *Official Journal of the European Union L 119/1* – GDPR.

[51] Gde su propisane novčane kazne do najvećeg iznosa od 20.000.000 € ili 4 % ukupnog godišnjeg prihoda u prethodnoj finansijskoj godini.

i krivične sankcije za nepoštovanje odredaba u svojim nacionalnim zakonima. Za sada je nejasno kako će članice EU sprovesti te odredbe, ali na ovaj način može doći do nekonzistentnog tretmana.[52]

DORA donosi niz izazova za poslovanje osiguravajućih društava, ali osiguravajuća društva koja budu uspela da se izbore sa ovim izazovima biće dobro pozicionirana za kontinuirani napredak u sve digitalnijem finansijskom i poslovnom okruženju.[53]

VI Zaključak

Poslovanje osiguravajućih društava u digitalnom okruženju predstavlja dinamičan i sveobuhvatan proces transformacije koji obuhvata tehnološke inovacije, promene u poslovnim modelima i prilagođavanje novim očekivanjima klijenata. Digitalizacija osiguravajućim društvima omogućava povećanje efikasnosti, smanjenje troškova, te poboljšanje korisničkog iskustva kroz brže i personalizovanije usluge. Međutim, imajući u vidu da takvo poslovanje sa sobom nosi i niz rizika, a da je potrebno prevazići fragmentaciju tržišta koja nastaje usled različitih zakonodavnih rešenja zemalja članica, na nivou EU doneta je DORA. Uopšteno gledano, DORA predstavlja značajan korak napred u poboljšanju digitalne operativne otpornosti osiguravajućih društava, kao i ostalih finansijskih institucija u EU. Međutim, ona pred ta društva postavlja i značajne izazove, uključujući potrebu za proširenjem sposobnosti njihove operativne otpornosti, uspostavljanjem posebne kontrolne funkcije za upravljanje IKT rizicima, unapređenjem sposobnosti izveštavanja o incidentima i razvojem sofisticiranijih metoda testiranja i analize scenarija. Osim toga, kompanije će morati značajno da ulažu u edukaciju osoblja, unapređenje komunikacije sa partnerima, klijentima, nadzornim telom.

Da bi uspešno primenila novu regulativu, osiguravajuća društva treba da preduzmu niz koraka. Najpre je potrebno da investiraju u IT infrastrukturu jer samo kontinuirana ulaganja u modernu i sigurnu IT infrastrukturu mogu obezbediti uspešnu digitalnu transformaciju. Osim toga neophodno je da izvrše obuke zaposlenih kako bi omogućili bolje razumevanje i primenu sigurnosnih mera i procedura. Dodatno im primenu može olakšati saradnja i angažovanje eksternih stručnjaka, što će olakšati i identifikaciju i otklanjanje slabosti u sigurnosnim sistemima. Redovno testiranje otpornosti i simulacije incidenta omogućavaju bolje pripreme za realne pretnje.

Osiguravajuća društva koja uspešno integrišu digitalne tehnologije u svoje poslovanje imaju potencijal da značajno unaprede svoju konkurentnost na tržištu, te da pruže kvalitetnije i efikasnije usluge svojim klijentima. Digitalno okruženje ne

[52] T. Ammann, I. Syed, V. Sanchez, 45.

[53] Pavel Gusiv, *Development of a Compliance Gap Analysis Method For The Digital Operational Resilience Act (DORA)*, master rad, Lapland University of Applied Scciences, 2023, 29.

samo da transformiše način na koji posluju već i otvara nove prilike za inovacije i rast u delatnosti osiguranja. U tom aspektu, postojanje detaljne regulative za obezbeđivanje digitalne operativne otpornosti biće im od posebnog značaja.

Literatura

- Ammann, T., Syed, I., Sanchez, V., „Exploring Operational Resilience in Financial Services – the Effects of DORA on Risk and Regulation in Top 3 Financial Markets", *Computer Law Review International*, 2/2023, 43-48.
- Barroso, L., „Fintechs: Concept, Level Playing Field and the Supervisory Approach", *Fintech Regulation and the Licensing Principle*, 2023, 25-44.
- Clausmeier, D., „Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)", *International Cybersecurity Law Review,* 4/2023, 79-90.
- Draft Regulatory Technical Standards on the Content of the Notification and Reports for Major Incidents and Significant Cyber Threats and Determining the Time Limits for Reporting Major Incidents and Draft Implementing Technical Standards on the Standard Forms, Templates and Procedures for Financial Entities to Report a Major Incident and to Notify a Significant Cyber Threat, https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_ _Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf, 20.07.2024.
- Draft Regulatory Technical Standards to Further Harmonise ICT Risk Management Tools, Methods, Processes and Policies as Mandated Under Articles 15 And 16(3) of Regulation (EU) 2022/2554, JC 2023 86, 2024, https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-_Final_report_on_draft_RTS_on_ICT_Risk_Management_Framework_and_on_simplified_ICT_Risk_Management_Framework.pdf, 25.07.2024.
- European Insurance and Occupational Pensions Authority (EIOPA), *Smernice o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija,* EIOPA-BoS-20/600.
- Federal Financial Supervisory Authority (Bafin), „Supervisory Requirements for IT in Insurance Undertakings", 2022.
- Grima, S., Marano, P., „Designing a Model for Testing the Effectiveness of a Regulation: The Case of DORA for Insurance Undertakings", *Risks*, 9/2021, 206-217.
- Gusiv, P., Development of a Compliance Gap Analysis Method For the Digital Operational Resilience Act (DORA), master rad, Lapland University of Applied Scciences, 2023.

- Kourmpetis, S., „Management of ICT Third Party Risk Under the Digital Operational Resilience Act", *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, Palgrave Macmillan, 2023, 211-226.
- Krüger, P. S., Brauchle, J.P., *The European Union, Cybersecurity, and the Financial Sector: A Primer*, Cyber Policy Initiative Working Paper Series – „Cybersecurity and the Financial System", Carnegie Endowment for International Peace , 2021.
- Kočević, J. et al., „Pravci razvoja tržišta osiguranja", *Tokovi osiguranja*, 3/2024, 536-548.
- Marano, P., Siri, M., „Regulating Insurtech in The European Union", *Journal of Financial Transformation,* 2021, 166-177.
- Martínez Resano, J. R., „Digital Resilience and Financial Stability – the Quest for Policy Tools in the Financial Sector", *Revista de Estabilidad Financiera*, 2022, 59-88.
- Pelc, P., „The Role of Cybersecurity in the Public Sphere - the European Dimension. Financial Institutions", in: *The Role of Cybersecurity in the Public Sphere – The European Dimension* (eds. K. C. Jentkiewicz, I. Hoffman), Maribor, 2022, 59-69.
- Risimović, M. Đurić, Z., Đurić, N. „Poslovanje sektora osiguranja u Republici Srbiji u uslovima pandemije kovida 19", *Tokovi osiguranja*, 1/2022, 111-148.
- Senabre, S., Soto, I. Munera, J., „Strengthening the Cyber Resilience of the Financial Sector - Developments and Trends", Financial Stability Review, 2021, 86-102.