Upravljanje rizicima informacijske tehnologije u uslugama osiguranja

Mazalin, Tina

Završni Specijalistički rad izrađen je na Sveučilištu u Zagrebu na Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog studija Informacijska sigurnost.

Mentor: izv. prof. dr. sc. Marin Vuković
Specijalistički rad ima: 57 stranica
Specijalistički rad br.: _____

Povjerenstvo za ocjenu u sastavu:

1. izv. prof. dr. sc. Miljenko Mikuc – predsjednik

2. izv. prof. dr. sc. Marin Vuković – mentor

3. izv. prof. dr. sc. Krešimir Grgić, Sveučilište Josipa Jurja Strossmayera u Osijeku Fakultet elektrotehnike, računarstva i informacijskih tehnologija - član

Povjerenstvo za obranu u sastavu:

1. izv. prof. dr. sc. Miljenko Mikuc – predsjednik

2. izv. prof. dr. sc. Marin Vuković – mentor

3. izv. prof. dr. sc. Krešimir Grgić, Sveučilište Josipa Jurja Strossmayera u Osijeku Fakultet elektrotehnike, računarstva i informacijskih tehnologija - član

Datum obrane: 6. veljače 2023.

SAŽETAK

Povodom novih pravnih zahtjeva u području mrežnih i informacijskih sustava u svrhu osiguravanja visoke razine digitalne operativne otpornosti za financijski sektor na razini Europske unije, cilj rada je analiza regulatornog okvira za postizanje kibersigurnosti u financijskom sektoru.

Posebno se analiziraju sigurnosni zahtjevi za uspostavu okvira upravljanja rizicima informacijsko komunikacijskih tehnologija, mjera za zaštitu, sprječavanje, otkrivanje i upravljanje incidentima, posebne obveze u svezi testiranja digitalne operativne otpornosti, izrada planova za odgovor i oporavak nakon incidenta, mjere za upravljanje rizicima informacijsko komunikacijskih tehnologija trećih strana i obveze financijskih subjekata u odnosu na razmjenu informacija o incidentima s nadležnim tijelima sukladno novom regulatornom okviru.

Budući da nadzorna tijela sektorskim zakonodavnim aktima već propisuju određene nužne zahtjeve za upravljanje u području informacijskih i komunikacijskih tehnologija, novi regulatorni okvir trebao bi se temeljiti na već uspostavljenim okvirima kibersigurnosti financijskih institucija i dodatno pridonijeti harmonizaciji pravila o digitalnoj operativnoj otpornosti država članica.

Ključne riječi: informacijska sigurnost, NIS2, DORA, rizik, kiberincident, regulatorno, osiguranje, informacijske tehnologije

ABSTRACT

Given the new regulatory requirements for the security of network and information systems, the aim of which is to ensure a high level of digital operational resilience for the financial sector at the level of the European Union, this paper is to analyze the regulatory framework on cybersecurity applicable in the financial sector.

This analysis includes the security requirements in regard with risk management framework for information and communication technologies, measures for protection, prevention, detection and management of incidents, specific obligations regarding digital operational resilience testing, response and recovery plans after an incident, oversight framework of critical ICT third-party service providers, and obligations on reporting of ICT incidents in accordance with new regulatory framework.

Since some financial entities already do have respective sector specific legislation on information and communication technology security and governance, further improvements within financial entities should be based on the already established security frameworks and additionally contribute to the harmonization of rules on digital operational resilience among different member states.

Keywords: information security, NIS2, DORA, risk, cyberincident, regulatory, insurance, information technology

SADRŽAJ

1. UVOD

Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (dalje u tekstu: Direktiva NIS) [1] donesena je 2016. godine i bila je prvi regulatorni okvir na razini Europske unije kojim se utvrdila obveza država članica da izrade strategije nacionalne kibersigurnosti koje će osigurati povećanje kiberotpornosti u odabranim sektorima i kod pružanja pojedinih digitalnih usluga, te obveza na uspostavu sustava za razmjenu informacija između tijela Europske unije, odnosno obveza utvrđivanja zahtjeva za uspostavu kibersigurnosti i prijavljivanje prepoznatih incidenata.

U svrhu donošenja mjera za daljnje povećanje otpornosti i kapaciteta svih dionika za pružanje odgovora na incidente u području kibersigurnosti i zaštiti kritične infrastrukture, u prosincu 2020. godine Europski parlament i Vijeće donijeli su Prijedlog Direktive Europskog parlamenta i vijeća o mjerama za visoku zajedničku razinu kibersgurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 (dalje u tekstu: Prijedlog Direktive NIS 2) [2]

Pravila o digitalnoj operativnoj otpornosti u financijskom sektoru diljem Europske unije trenutno se pronalaze u zasebnim sektorskim smjernicama nadzornih tijela kao što su Europsko nadzorno tijelo za bankarstvo (dalje u tekstu: EBA), Europsko nadzorno tijelo za vrijednosne papire i tržište kapitala (dalje u tekstu: ESMA) i Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje (dalje u tekstu: EIOPA).

Zbog manjka harmoniziranih i sveobuhvatnih pravila o digitalnoj operativnoj otpornosti na razini Europske unije prepoznata je potreba za uspostavom zajedničkog pristupa država članica u osiguravanju kiberotpornosti financijskog sektora.

U radu se provodi usporedna analiza postojećeg regulatornog okvira o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija u odnosu na društva za osiguranje i novih jedinstvenih pravila za postizanje digitalne operativne otpornosti kod financijskih subjekata.

Cilj rada je utvrditi minimalne regulatorne zahtjeve u svrhu implementacije sigurnosnih mjera u poslovne procese društva za osiguranje radi osiguravanja učinkovite i visoke razine zaštite digitalne operativne otpornosti.

U narednom poglavlju analizirati će se područje primjene novih propisa za postizanje visoke razine kibersigurnosti i digitalne operativne otpornosti i smjernica EIOPA-e. Ujedno će se analizirati različita tumačenja osnovnih pojmova informacijske sigurnosti koji su od važnosti za ovaj rad. U četvrtom poglavlju analiziraju se sigurnosni zahtjevi za postizanje digitalne operativne otpornosti koji bi trebali biti sastavni dio implementacijskog projekta društva za osiguranje u svrhu postizanja usklađenosti s novim regulatornim okvirom. U petom poglavlju analizira se novi regulatorni okvir kibersigurnosne certifikacije proizvoda, usluga i procesa. U šestom poglavlju analizira se primjer izdvajanja poslova društva za osiguranje trećoj strani pružatelju usluga računarstva u oblaku. U sedmom poglavlju navedeni su zaključci o utjecaju novog regulatornog okvira na sigurnost IKT društva za osiguranje.

2. REGULATORNI OKVIR

U svrhu poboljšanja postojećih mjera kibersigurnosti, u prosincu 2020. godine donesen je Prijedlog Direktive NIS 2 [2] kao rezultat *ex post* evaluacija, savjetovanja s dionicima i procjene učinka koji u bitnom ističu niže navedene argumente [2].

Razlog donošenja novog akta je potreba modernizacije postojećeg pravnog okvira uzimajući u obzir digitalizaciju unutarnjeg tržišta i sve veće kibersigurnosne prijetnje te rast broja sofisticiranih kibernapada dodatno potenciranih pandemijom COVID-19. Provedenom procjenom učinka uočeni su sljedeći problemi: „(1) niska razina kiberotpornosti poduzeća koja posluju u Europskoj Uniji; (2) neujednačena otpornost u državama članicama i sektorima i (3) niska razina zajedničke informiranosti o stanju te nedostatak zajedničkog odgovora na krizu.“ [2]

U svrhu smanjenja regulatornog opterećenja za nadležna tijela i javne i privatne subjekte predviđeno je ukidanje obveze nadležnih tijela da samostalno utvrđuju operatore ključnih usluga, harmonizacija sigurnosnih zahtjeva i izvješćivanja i harmonizacija prekogranične provedbe.

U odnosu na dosljednost s drugim aktima, Prijedlog Direktive NIS 2 [2] dio je šireg skupa postojećih i nadolazećih pravnih instrumenata, među kojima su i novi regulatorni propisi u području digitalne operativne otpornosti za financijski sektor koji će se nakon stupanja na snagu smatrati kao *lex specialis* u odnosu na Prijedlog Direktive NIS 2 [2].

Donošenje novih propisa razmjerno je sve većim rizicima i potrebi osiguravanja kontinuiteta i kvalitete usluga te povezanim troškovima za poboljšanje postojećeg okvira koji su mali u

odnosu na moguću štetu uzrokovanu kiberincidentima. Dodatno, kao objašnjenje za donošenje direktive, a ne uredbe (koje odredbe bi se izravno primjenjivale u svim državama članicama) navodi se potrebna fleksibilnost država članica u određivanju ključnih i važnih subjekata i radu nadležnih tijela [2].

Rezultati ispitivanja funkcioniranja Direktive NIS [1], *ex post* evaluacije, savjetovanja i provedene procjene učinka sukladno prijedlogu, u bitnom čine sljedeće [2]:

- ograničen broj sektora na koje se primjenjuje Direktiva NIS [1];
- nejasna primjena za operatore ključnih usluga i pružatelje digitalnih usluga;
- različitost u utvrđivanju zahtjeva sigurnosti i izvješćivanja o incidentima između država članica;
- neučinkovit sustav nadzora i provedbe;
- različitost u financijskim i ljudskim resursima;
- manjak sustavne razmjene informacija između dionika.

Nadalje, kako se navodi u Prijedlogu Direktive NIS 2 [2], Europska komisija razmotrila je tri opcije za poboljšanje pravnog okvira u području kiberotpornosti i odgovora na incidente, te se odlučila na opciju sustavne i strukturne promjene Direktive NIS[1].

Dogovor o novim propisima postignut je nakon završetka međuinstitucijskih pregovora 13. svibnja 2022. godine.

Budući da je u idućim mjesecima planirano formalno usvajanje Prijedloga Direktive NIS 2 [2] te da u trenutku pisanja ovog rada još uvijek nije izdan prijevod postignutog dogovora na hrvatski jezik, u ovom radu analizirati će se prijedlog usuglašenog teksta, u slobodnom prijevodu autora, kako stoji u *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148* od 17. lipnja 2022 [3]

Kako je navedeno u Komunikaciji Komisije Europskom parlamentu, Vijeću, Europskoj središnjoj banci, europskom gospodarskom socijalnom odboru i odboru regija [4] u sklopu akcijskog plana za financijske tehnologije (*eng. FinTech*), Europska komisija pozvala je europska nadzorna tijela EIOPA-u, EBA-u i ESMA-u na analizu i utvrđivanje prakse nadzornih tijela na financijskom tržištu u odnosu na sigurnost informacijsko komunikacijskih tehnologija (dalje u tekstu: IKT), donošenje smjernica za upravljanje rizicima IKT te ih je pozvala na pružanje savjeta Europskoj komisiji o potrebnim legislativnim promjenama.

Nakon analize postojećeg zakonodavstva o generalnoj operativnoj otpornosti financijskog sektora, uključujući i upravljanje rizicima IKT, 10. travnja 2019. godine, EIOPA, EBA i ESMA izdale su Zajednički tehnički savjet (*eng. Joint Advice of the European Supervisory Authorities*) [5]. Prijedlog nadzornih tijela odnosio se na nužnu uspostavu općih zahtjeva upravljanja rizicima IKT u odnosu na sve relevantne subjekte, harmonizaciju izvještavanja o incidentima IKT i upravljanje rizicima IKT s trećim stranama pružateljima usluga IKT.

Prijedlog Uredbe Europskog parlamenta i vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) donesen je 24.09.2020. (dalje u tekstu: Prijedlog Uredbe DORA) [6].

Nastavno na donesen Prijedlog Uredbe DORA [6], nadzorna tijela izdale su službeno priopćenje u kojem su podržale harmonizaciju regulatornih okvira Europske unije radi postizanja digitalne operativne otpornosti financijskog rizika.

Europska federacija osiguratelja i reosiguratelja *(eng. Insurance Europe)* među ostalim, pozvala je Europsku komisiju [7] na izmjene Prijedloga Direktive NIS 2 [2] u kojima će se u konačnom tekstu jasnije utvrditi obveznici primjene i isključenje društva za osiguranje budući da je istovremeno u tijeku donošenje novih propisa, odnosno Prijedlog Uredbe DORA [6], a koja se ima smatrati *lex specialis* propisom.

Predsjedništvo Vijeća i Europski parlament postignuli su privremeni dogovor o novim pravilima o digitalnoj operativnoj otpornosti 11. svibnja 2022. godine [8]. Budući da je u narednim mjesecima planirano formalno usvajanje Prijedloga Uredbe DORA [6], te da u trenutku pisanja ovog rada još uvijek nije izdan prijevod postignutog dogovora na hrvatski jezik, u ovom radu analizirat će se prijedlog usuglašenog teksta, u slobodnom prijevodu autora, kako je isti naveden u *Provisional agreement resulting from interinstitutional negotitations: Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014* [8].

3. MJERE ZA VISOKU ZAJEDNIČKU RAZINU KIBERSIGURNOSTI I DIGITALNE OPERATIVNE OTPORNOSTI ZA FINANCIJSKI SEKTOR

3.1. Područje primjene Prijedloga Direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kiberisgurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148

U posljednjem Prijedlogu Direktive Europskog parlamenta i vijeća o mjerama za visoku zajedničku razinu kiberisgurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 (dalje u tekstu: Direktiva NIS-2) [3] utvrđuju se mjere čiji cilj je postizanje visoke zajedničke razine kibersigurnosti u Europskoj uniji kako bi se poboljšalo funkcioniranje unutarnjeg tržišta.

Obveznici primjene Direktive NIS-2 [3] obvezni su uspostaviti upravljanje kibersigurnosnim rizicima i izvješćivati o njima te se ista primjenjuje na javne i privatne subjekte koji zadovoljavaju ili prelaze kriterij malih i srednjih subjekata. Ključnim subjektima smatraju se oni iz područja energetike, prometa, zdravlja, vode za piće, otpadnih voda, javne uprave, bankarstva i digitalne infrastrukture sukladno kriterijima i iznimkama navedenim u Prilogu 1 Direktive NIS-2 [3]. Kao obveznici primjene uvode se i važni subjekti pružatelji poštanskih i kurirskih usluga, gospodarenja otpadom, izrada, proizvodnja i distribucija kemikalija, proizvodnja i distribucija hrane, proizvodnja i pružatelji digitalnih usluga sukladno kriterijima i iznimkama navedenim u Prilogu 2 Direktive NIS-2 [3].

Neovisno o veličini subjekta, Direktiva NIS-2 [3] primjenjuje se i na ključne i važne subjekte pružatelje javnih elektroničkih mreža, pružatelje usluga povjerenja i registre naziva vršnih domena i pružatelje usluga sustava naziva domena (DNS).

Područje primjene Uredbe Europskog parlamenta i Vijeća o digitalnoj i operativnoj otpornosti za financijski sektor

Europski parlament i Vijeće uskladili su tekst Direktive NIS-2 [3] sa Uredbom o digitalnoj i operativnoj otpornosti za financijski sektor (dalje u tekstu: Uredba DORA) u odnosu na obveze financijskih institucija da osiguraju digitalnu operativnu otpornost kako bi postigli jasnoću i usklađenost Direktive NIS-2 [3] i Uredbe DORA [8] kao sektorskog propisa koji se primjenjuje *lex specialis* u odnosu na subjekte financijskog sektora. Navedeno proizlazi i iz uvodne izreke broj 13 Direktive NIS-2 [3] prema kojoj se ista ne primjenjuje na financijske subjekte koji su obveznici primjene Uredbe DORA [8].

Istovremeno, sukladno odredbama Uredbe DORA [8], europska nadzorna tijela (dalje u tekstu: ESA) i nacionalna nadležna tijela zadužena za financijski sektor sudjeluju u radu Skupine za suradnju, razmjenjuju informacije i surađuju s jedinstvenim kontaktnim točkama i s nacionalnim CSIRT-ovima sukladno Direktivi NIS-2 [3] i to osobito u odnosu na razmjenu informacija o velikim IKT incidentima i povezanim i značajnim kibernetičkim prijetnjama.

Budući da je Uredba DORA [8] kao zakonodavni akt uredba, za razliku od Direktive NIS-2 [3], ona propisuje jedinstvene sigurnosne zahtjeve mrežnih i informacijskih sustava financijskih subjekata koji se izravno primjenjuju u cijeloj Europskoj uniji i čijom primjenom je potrebno postići visoku zajedničku razinu digitalne operativne otpornosti. Treba primijetiti i kako Direktiva NIS-2 [3] i Uredba DORA [8] od ključnih i važnih subjekata, odnosno financijskih subjekata, očekuju visoku razinu kibersigurnosti odnosno visoku razinu digitalne operativne otpornosti.

Financijski subjekti kao obveznici primjene Uredbe DORA [8] obvezni su uspostaviti upravljanje rizicima IKT, izvještavanje o incidentima i kiberprijetnjama IKT, te ispuniti minimalne sigurnosne zahtjeve u odnosima s trećim stranama pružateljima uslugama IKT i nadzornim tijelima.

Sukladno članku 2, Uredba DORA [8] primjenjuje se na kreditne institucije, institucije za platni promet (sukladno iznimkama u članka 32 stavak 1 Direktive (EU) 2015/2366 [9]), pružatelje usluga informacija o računu, institucije za elektronički novac, investicijska društva, pružatelje usluga povezanih s kriptoimovinom i izdavatelje tokena vezanih uz kriptoimovinu, središnje depozitorije vrijednosnih papira, središnje druge ugovorne strane, mjesta trgovanja, upravitelje alternativnih investicijskih fondova, društva za upravljanje, pružatelje usluga dostave podataka, društva za osiguranje i reosiguranje, posrednike u osiguranje i posrednike u reosigurnaju i sporedne posrednike, institucije za strukovno mirovinsko osiguranje, agencije za kreditni rejting, administratore ključnih referentnih vrijednosti, pružatelje usluga skupnog financiranja, sekuritizacijske repozitorije i treće strane pružatelje usluga IKT.

Nadalje, sukladno članku 2 stavak 3 točka b), Uredba DORA [8] ne primjenjuje se na društva za osiguranje i reosiguranje kako su isti navedeni u članku 4. Direktive 2009/138/EZ [10] te na društva za osiguranje i reosiguranje odnosno posrednike u osiguranje koji su mikro poduzetnici ili mali ili srednji poduzetnici.

3.2. Područje primjene smjernica Europskog nadzornog tijela za osiguranje i strukovno mirovinsko osiguranje

U skladu s Uredbom (EU) br. 1094/2010 [11] nadležna tijela i financijske institucije uključujući društva za osiguranje, uz primjenu nacionalnih propisa, obvezna su uložiti sve napore kako bi poštivala smjernice i preporuke EIOPA-e.

Smjernice o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija (dalje u tekstu: Smjernice EIOPA-e o sigurnosti IKT) [12] kao osnovni cilj navode: „osigurati pojašnjenja i transparentnost za sudionike na tržištu u vezi s najmanjim očekivanim kapacitetima u području informacijske sigurnosti i kibersigurnosti, tj. osnovnom razinom sigurnosti; spriječiti potencijalnu regulatornu arbitražu; poticati nadzornu konvergenciju s obzirom na očekivanja i postupke primjenjive u vezi s upravljanjem i sigurnosti u području IKT-a kao ključ za pravilno upravljanje sigurnosnim rizicima i rizicima IKT-a“ [12]

3.3. Tumačenje pojmova

3.3.1. Mrežni i informacijski sustav

Budući da je Direktiva 2002/21/EZ [13] stavljena izvan snage 20.10.2020.godine Direktiva NIS 2 [3] izmijenila je definiciju „mrežnih i informacijskih sustava“ u odnosu na definiciju iz Direktive NIS [1].

Sukladno članku 4 stavak 1 točka (a) Direktive NIS-2 [3], mrežni i informacijski sustavi znači „elektronička i komunikacijska mreža u smislu članka 2 stavak 1 Direktive 2018/1972“ odnosno „sustavi prijenosa, bez obzira na to temelje li se na stalnoj infrastrukturi ili centraliziranom upravljačkom kapacitetu, i, ako je to primjenjivo, opremu za prespajanje ili usmjeravanje te druga sredstva, uključujući mrežne elemente koji nisu aktivni, a koji dopuštaju prijenos signala žičanim, radijskim, optičkim ili drugim elektromagnetskim sredstvom, što uključuje satelitske mreže, zemaljske nepokretne (s prespajanjem kanala, prespajanjem paketa podataka, uključujući internet) i pokretne mreže, elektroenergetske kabelske sustave, u mjeri u kojoj se rabe za prijenos signala, mreže koje se rabe za radijsku i televizijsku radiodifuziju te mreže kabelske televizije, bez obzira na vrstu informacija koju prenose“.

Nadalje, mrežni i informacijski sustav sukladno članku 4 stavak 1 (b) i (c) Direktive NIS-2 [3] uključuje i svaki uređaj ili skupinu povezanih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka, te digitalne podatke koji se tim uređajima ili putem elektroničke komunikacijske mreže pohranjuju, obrađuju, dobivaju ili prenose.

3.3.2. Sigurnost mrežnih i informacijskih sustava

Sukladno članku 4 stavak 2 Direktive NIS-2 [3] mijenja se definicija „sigurnosti mrežnih i informacijskih sustava“ u odnosu na Direktivu NIS [1]. Nova definicija glasi: „sigurnost mrežnih i informacijskih sustava znači sposobnost mrežnih i informacijskih sustava da odolijevaju na određenoj razini pouzdanosti svakom događaju koji može ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjeni ili prenesenih ili obrađenih podataka ili srodnih usluga koji ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup“ [3].

Iz ovog je jasno da je već u samoj definiciji sigurnosti mrežnih i informacijskih sustava proširen opseg mogućih utjecaja na sigurnost i podignut ciljani prag sigurnosti budući da se naglasak stavlja na potencijalnu ugrozu u odnosu na već postojeću ugrozu prema čemu su obveznici primjene nužni prepoznati svaki događaj koji bi mogao ugroziti tražene zahtjeve u odnosu na ranije postojeće radnje kojima se ugrožavaju zahtjevi dostupnosti, autentičnosti, cjelovitost ili povjerljivosti.

S druge strane, definicija „mrežnih i informacijskih sustava“ sukladno članku 3 točka (2) i definicija „sigurnosti mrežnih i informacijskih sustava“ sukladno članku 3 točka (3) Uredbe DORA [8] poziva se na definicije kako su navedene u Direktivi NIS [1] odnosno Direktivi 2002/21/EZ koja je već stavljena izvan snage 2020. godine.

Budući da se donošenjem Direktive NIS-2 [3], Direktiva NIS [1] stavlja izvan snage, te da su pojmovi „mrežni i informacijski sustav“ te „sigurnost mrežnih i informacijskih sustava“ izmijenjeni Direktivom NIS-2 [3], treba primijeniti da se ovdje radi o nedosljednosti u definiranju ovih pojmova u Uredbi DORA [8] te je pretpostavka da bi iste trebalo tumačiti u skladu s novim definicijama sukladno članku 4 Direktive NIS-2 [3] kako su iste gore navedene.

Nadalje, sukladno Smjernicama EIOPA-e o sigurnosti IKT [12] „kibersigurnost znači očuvanje povjerljivosti, cjelovitosti i dostupnosti informacija i/ili informacijskih sustavâ putem kibernetičkog medija“, a „informacijska sigurnost“ definira se kao „očuvanje povjerljivosti, cjelovitosti i dostupnosti informacija i/ili informacijskih sustava. Usto može obuhvaćati i autentičnost, odgovornost, nepobitnost i pouzdanost.“

3.3.3. Ranjivost

Pojam „ranjivost“ različito se definira u gore analiziranim pravnim aktima. Naime, sukladno članku 4 točke (12) Uredbe DORA [8] „ranjivost znači slabost, osjetljivost ili mana nekog resursa, sustava, procesa ili kontrole koje mogu biti iskorištene“, dok Direktiva NIS-2 [3]

također povezuje pojam ranjivosti „slabost, osjetljivost ili manu“ s proizvodima ili uslugama IKT koje mogu biti iskorištene od strane kiberprijetnje. Smjernice EIOPA-e o sigurnosti IKT [12] definiraju ranjivost kao „slabost, podložnost ili manu imovine ili kontrolne funkcije koju može iskoristiti jedna prijetnja ili više njih“.

3.3.4. Rizik

Direktiva NIS-2 [3] mijenja i definiciju rizika u odnosu na Direktivu NIS [1] pa sukladno članku 7 točka (a) „rizik znači potencijalan gubitak ili poremećaj uzrokovan incidentom i treba se izraziti kao kombinacija ukupnog gubitka ili poremećaja i vjerojatnosti nastanka tog incidenta“.

Sukladno članku 3 točka (4) Uredba DORA [8] definira rizik IKT kao „bilo koja razumno prepoznatljivu okolnost u vezi s korištenjem mrežnih i informacijskih sustava koji, ako se materijaliziraju, mogu ugroziti sigurnost mreže i informacijskih sustava, bilo kojeg tehnološki ovisnog alata ili procesa u vezi operacija i procesa, ili pružanja usluga na način da proizvede negativne učinke u digitalnom ili fizičkom okruženju.“

Smjernice EIOPA-e o sigurnosti IKT [12] definiraju rizik IKT i sigurnosni rizik kao „podkategoriju operativnog rizika; rizik gubitaka uslijed povrede povjerljivosti, gubitka integriteta sustava i podataka, neprikladnosti ili nedostupnosti sustava i podataka ili nemogućnosti promjene IKT-a unutar razumnog roka i uz razumne troškove u slučaju promjene u okruženju ili promjene zahtjeva poslovanja (to jest prilagodljivosti). To obuhvaća kiberrizike i rizike informacijske sigurnosti koji proizlaze iz neadekvatnih ili neuspješnih internih postupaka ili vanjskih događaja, uključujući kibernapade ili neadekvatnu fizičku sigurnost“.

3.3.5. Incidenti

U odnosu na Direktivu NIS[1], Direktiva NIS-2 [3] stavlja niži prag za prepoznavanje incidenta te u odnosu na ranije traženi nastanak „stvarnog negativnog učinka na sigurnost“ sukladno članku 4 točka (5) Direktive NIS-2 [3] „incident znači svaki događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili srodnih usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup.“

Direktiva NIS-2 [3] uvodi i novu kategoriju „kiberincidenta velikog razmjera koji se odnosi na svaki incident čiji poremećaji prelaze mogućnosti države članice da na njega odgovore ili ima značajan učinak na dvije ili više država članica.“

Kategorizacija tri vrste incidenata prisutna je i u Uredbi DORA [8] koja razlikuje tri vrste incidenata.

Prva kategorija incidenta sukladno članku 3 točka (6) Uredbe DORA [8] je incident IKT koji „znači jedan ili više od strane financijskih institucija neplaniranih događaja koji ugrožavaju sigurnost mrežnih i informacijskih sustava i imaju negativan učinak na dostupnost, autentičnost, integritet ili povjerljivost podataka ili usluga koje pruža financijska institucija“. U odnosu na definiciju incidenta iz Direktive NIS-2 [3] primjećuje se da uz „događaje koji ugrožavaju zahtjeve sigurnosti“ izričito traži i postojanje „negativnog učinka“ kao posljedice tih događaja.

Druga kategorija incidenta sukladno članku 3 točka (7) Uredbe DORA [8] je značajan incident IKT koji „ima visoki negativan učinak na mrežni i informacijski sustav koji podupire kritične funkcije financijske institucije“ što u kontekstu ovog propisa svakako ima smisla obzirom na sigurnosne zahtjeve za postizanje digitalne otpornosti ključnih funkcija. Iz ovog jasno proizlazi da će pitanje značajnog incidenta IKT prvenstveno ovisiti o identifikaciji ključnih funkcija unutar same financijske institucije.

Treća kategorija incidenta sukladno članku 3 točka (7a) Uredbe DORA [8] je operativni ili sigurnosni incident koji je „povezan s plaćanjem koji ne mora nužno biti povezan s IKT i odnosi se na samo pojedine financijske institucije kao što su kreditne institucije, institucije za platni promet i institucije za elektronički novac i koji ima negativan učinak na povjerljivosti, integritet i dostupnost podataka ili na kontinuitet pružanja usluga plaćanja.“ Treba primijetiti da se kao negativan učinak koji proizlazi iz operativnog ili sigurnosnog incidenta ne navodi ugrožavanje autentičnosti podataka ili autentičnosti u pružanju usluga plaćanja. Iako ova vrsta incidenta ne mora nužno biti povezana s IKT, financijske institucije trebale bi osigurati zaštitu autentičnosti podataka, a osobito provjeru autentičnosti osoba u pružanju usluga plaćanja.

Konačno, Smjernice EIOPA-e o sigurnosti IKT [12] definiraju operativni ili sigurnosni incident kao „jedan događaj ili niz povezanih neplaniranih događaja koji imaju ili će vjerojatno imati negativan učinak na cjelovitost, dostupnost, i povjerljivost sustava i usluga IKT-a.“

3.3.6. Društvo za osiguranje

Sukladno članku 3 točka (34) DORA-e [8] u primjeni su definicije iz Direktive o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja 2009/138/EZ (Direktiva o solventnosti II) [10] i Direktive o distribuciji osiguranja (EU) 2016/97 [14] prema kojima; društvo za osiguranje je „društvo izravno životno ili neživotno osiguranje koje je dobilo odobrenje za rad, društvo za reosiguranje znači ono društvo koje je dobilo odobrenje za obavljanje djelatnosti reosiguranja te posrednik za osiguranje znači svaka fizička ili pravna osoba, osim društva za osiguranje ili

društva za reosiguranje ili njegovih zaposlenika i osim sporednog posrednika u osiguranju, koja za naknadu osniva ili obavlja poslove distribucije osiguranja“

Sporedni posrednik u osiguranju znači „svaka fizička ili pravna osoba, osim kreditnih institucija ili investicijskih društava koja za naknadu osniva ili obavlja poslove distribucije osiguranja kao sporednu djelatnost“

Posrednik u reosiguranju znači „svaka fizička ili pravna osoba, osim društva za reosiguranje ili njegovih zaposlenika, koji za naknadu osnivaju ili obavljaju poslove distribucije reosiguranja.“

3.3.7. Digitalna operativna otpornost

Sukladno članku 3 točka (1) Uredbe DORA [8] definicija digitalne operativne otpornosti znači „sposobnost financijskog subjekta da izgradi, osigura i preispita svoj operativni integritet s tehnološkog aspekta osiguravajući, izravno ili neizravno, korištenjem usluga trećih strana pružatelja usluga IKT, cijeli dijapazon kapaciteta koji se odnose na IKT i potrebni su za sigurnost mrežnih i informacijskih sustava koje financijski subjekt koristi te koji podržavaju kontinuirano pružanje financijskih usluga i njihovu kvalitetu“.

Iz ove definicije sažeto proizlaze konačni ciljevi koje bi financijski subjekti trebali ostvariti: prvo, sposobnost uspostave, osiguravanja i preispitivanja operativnog integriteta i pouzdanosti; drugo, potpuni kapacitet usluga IKT radi osiguravanja sigurnosti mreže i informacijskog sustava; treće, kontinuitet poslovanja i kvalitetu za vrijeme remećenja ili prekida.

3.3.8. Načelo proporcionalnosti

Kao temeljno načelo u uspostavi procesa digitalne operativne otpornosti, Uredba DORA [8] navodi načelo proporcionalnosti kojim bi se trebali voditi financijski subjekti pri implementaciji sigurnosnih zahtjeva, te nadležna tijela u provođenju nadzora. Načelo proporcionalnosti podrazumijeva implementaciju zahtjeva u skladu s veličinom, prirodom, opsegom i složenosti usluga, aktivnosti i operativnih radnji i u skladu s njihovim generalnim profilom rizika.

Načelo proporcionalnosti u upravljanju rizicima IKT u osiguravajućim društvima temeljno je načelo i sukladno Smjernicama EIOPA-e o sigurnosti IKT [12] sukladno kojemu društva za osiguranje moraju isto primijeniti i kod uspostave službe za informacijsku sigurnost i imenovanja odgovorne osobe, uspostavi postupaka za logičku kontrolu pristupa i logičku sigurnost (gdje bi se aktivnosti korisnika trebale pratiti na način proporcionalan riziku),

određivanju ugovornih obveza radi osiguravanja proporcionalnih ciljeva i kod primjene mjera sigurnosti u slučajevima izdvajanja poslova u vezi s kritičnim ili važnim funkcijama.

Načelo proporcionalnosti temeljno je načelo i u Direktivi o solventnosti II [10] i Ugovoru o funkcioniranju Europske unije [15] te se u svim gore navedenim propisima primjenjuje na dvije razine; na razini provođenja nadzora obveznika primjene i na razini uspostave usklađenosti od strane obveznika primjene uzimajući u obzir prirodu, opseg i složenost rizika prisutnih u poslovanju društva za osiguranje odnosno društva za reosiguranje.

Sukladno navedenim propisima primjena načela proporcionalnosti u uspostavi sigurnosnih zahtjeva podrazumijeva provođenje procjene rizika na način da sustav upravljanja bude proporcionalan riziku te istovremeno omogućuje odgovarajući nadzor i evaluaciju rizika neovisno o tome je li izvor rizika vanjski ili unutarnji.

Načelo proporcionalnosti jasno se očituju i u odredbama Uredbe DORA [8] koja razlikuje obveze velikih financijskih subjekata (kojima nameće obvezne zahtjeve ili zahtjeve s višim stupnjem odgovornosti) i mala i srednja poduzeća te mikropoduzeća koji podliježu manje strogim zahtjevima (*eng. light framework*). Upravo primjenom načela proporcionalnosti Uredba DORA [8] je kao obveznike primjene isključila ista ona društva za osiguranje i reosiguranje koji su isključeni od primjene Direktive o solventnosti II sukladno članku 4 [10].

Preostaje vidjeti kako će se načelo proporcionalnosti tumačiti kod implementacije sigurnosnih zahtjeva Uredbe DORA [8] budući da nisu uvijek utvrđeni minimalni sigurnosni zahtjevi nego razna obvezne zaštite ovisi o testovima ravnoteže i procjenama rizika i učinka koje moraju provesti samostalno financijski subjekti. To ujedno znači da će financijski subjekti morati dokumentirati proces donošenja odluka o mjerama odabrane zaštite.

4. ZAHTJEVI ZA POSTIZANJE DIGITALNE OPERATIVNE OTPORNOSTI OSIGURAVAJUĆEG DRUŠTVA

U svrhu implementacijskog projekta usklađivanja poslovnih procesa financijskih subjekata sa sigurnosnim zahtjevima iz Uredbe DORA [8] potrebno je sastaviti projektni tim i projektni plan prema jednoj od opće poznatih metodologija ili sukladno internim pravilima i metodologiji financijskog subjekta koja se primjenjuje u odnosu na regulatorna usklađenja. Neovisno o odabranom modelu provođenja implementacije, svaki projektni plan trebao bi sadržavati odluku upravljačkog tijela o provođenju projekta koju čine obrazloženje, utjecaj na poslovanje, opseg projekta, ciljevi projekta, faze projekta, vrste i količina procijenjenih resursa, rokovi i

podaci o nositelju projektnog plana. Obzirom na prirodu projekta izvjesno je da će u konkretnom slučaju nositelj projektnog plana biti voditelj informacijske sigurnosti ili povezana organizacijska jedinica. Uzimajući u obzir da se u konkretnom slučaju radi u usklađenju postojećih poslovnih procesa s regulatornim zahtjevima, projektni plan trebao bi sadržavati barem dvije faze. U prvoj fazi, nakon utvrđivanja uloga i odgovornosti članova implementacijskog tima, trebalo bi utvrditi opseg i metodologiju za provođenje gap analize kako bi financijski subjekt utvrdio trenutni stupanj usklađenosti poslovanja s odredbama Uredbe DORA [8] i to osobito iz razloga što bi osiguravajuća društva već trebala imati uspostavljene procese za upravljanje sigurnosti u području informacijskih i komunikacijskih tehnologija. Gap analizu trebala bi provesti interna ili vanjska revizija. Nakon provedene analize, utvrđivanja statusa i procjene rizike, potrebno je utvrditi ciljeve projekta, aktivnosti koje će biti obuhvaćene projektom, odnosno opseg projekta. Nositelj projekta trebao bi provesti prioritizaciju aktivnosti i sastaviti plan izvršavanja različitih tokova, utvrditi resurse i rokove za provedbu implementacije. Uzimajući u obzir da gap analiza i projektni plan sadrži pravne, sigurnosne, tehničke i procesne zahtjeve kao i sistematizaciju poslova, projektni tim barem bi trebali sačinjavati predstavnici organizacijske jedinice za (informacijsku) sigurnost, za informacijske tehnologije, za infrastrukturu IKT, za upravljanje rizicima, za komunikacije, za usklađenost ili pravne poslove. U projekt bi trebali biti uključeni i službenik za zaštitu osobnih podataka, kao i predstavnici svih organizacijskih jedinica poslovne strane, odnosno vlasnici podataka, ovisno o zahtjevima i aktivnostima pojedinog projektnog toka.

4.1. Odgovornost upravljačkog tijela

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 1-3 Uredbe DORA [8] *i Smjernicama EIOPA-e o sigurnosti IKT (smjernica broj 1, 8, 25)* [12].

Osnovni zahtjev odnosi se na obvezu financijskog subjekta na uspostavu okvira unutarnjeg upravljanja i kontrole kojim će se osigurati djelotvoran i razborit proces upravljanja svim rizicima IKT radi postizanja visoke razine digitalne operativne otpornosti.

Upravljačko tijelo krajnje je odgovorno za upravljanje rizicima IKT, što bi trebalo tumačiti na način da neovisno o internoj organizaciji i sistematizaciji poslova, odgovornost upravljanja rizicima IKT je na upravljačkom tijelu financijskog subjekta. Upravljačko tijelo snosi ukupnu odgovornost za uspostavu i odobravanje strategije digitalne operativne otpornosti i za utvrđivanje odgovarajuće razine tolerancije na rizik.

Potrebno je osvrnuti se i na zahtjev prema kojem financijski subjekt mora uspostaviti *„eng. effective and prudent managment of all ICT risks“* Naime, u trenutku pisanja ovog rada još uvijek nije izdan službeni prijevod Uredbe DORA [8] na hrvatski jezik, međutim ako za tumačenje pogledamo službeni prijevod Prijedloga Uredbe o digitalnoj operativnoj otpornosti za financijski sektor od 24.09.2020. [6] termin *“effective“* je preveden kao „djelotvoran“.

Međutim, sukladno Časopisu za kulturu hrvatskog književnog jezika [17] tumačenje bi se trebalo provoditi prema normama ISO 9000:2005, 3.2.14 i ISO 9000:2005, 3.2.15. odnosno hrvatskim normama koje izdaje Državni zavod za normative HRN EN ISO 9000:2008. Sukladno navedenom, ispravan prijevod pridjeva *eng. effectiveness* bio bi „učinkovitost“ (mjera u kojoj se ostvaruju planirane radnje i postižu planirani rezultati), a ne „djelotvornost“.

Učinkovitost kao mjera u kojoj se ostvaruju planirane radnje i postižu planirani rezultati bitno je drugačijeg značenja od pridjeva *eng. efficiency* koji se prevodi kao „djelotvornost“ i podrazumijeva postojanje odnosa između postignutih rezultata i upotrijebljenih resursa.

Naime, u kontekstu Uredbe DORA [8] odgovornost financijske institucije da uspostavi „učinkovit“ (a ne djelotvoran) sustav upravljanja rizicima IKT podrazumijeva i prethodnu analizu i postavljanje ciljeva koje takav sigurnosni sustav mora postići.

Nadalje, upravljačko tijelo obvezno je uspostaviti politike čiji cilj je održavanje visoke razine povjerljivosti, integriteta i dostupnosti podataka. U odnosu na Smjernice EIOPA-e o sigurnosti IKT [12], Uredba DORA [8] osim uspostave sustava naglašava i važnost održavanja istog što implicira niz drugih mjera i kontrola koje financijski subjekti moraju implementirati u svrhu praćenja unutarnjih i vanjskih promjena koje bi mogle imati utjecaj na postojeću razinu zaštite.

Smjernice EIOPA-e o sigurnosti IKT [12] predviđaju obvezu donošenja pisane politike informacijske sigurnosti koju odobrava upravno, upravljačko ili nadzorno tijelo i koja među ostalim sadrži opis glavnih uloga i odgovornosti za upravljanje informacijskom sigurnosti i odgovornost osoblja na svim razinama. Usporedno, Uredba DORA [8] propisuje odgovornost upravljačkog tijela da odredi jasne uloge i odgovornosti svih funkcija u području IKT i obvezu uspostave odgovarajućeg sustava upravljanja.

Sukladno Uredbi DORA [8] upravljačko tijelo ima obvezu odobriti, nadzirati i periodično preispitivati implementaciju plana kontinuiteta poslovanja IKT i planove odgovora i oporavka što je u potpunosti u skladu i sa Smjernicama EIOPA -e o sigurnosti IKT [12] koje propisuju uspostavu planova i njihovo testiranje i redovito ažuriranje. Uredba DORA [8] dodatno

utvrđuje izričitu obvezu upravljačkog tijela da odobri i periodično nadzire interne planove revizije IKT-a, revizije IKT-a i njihove bitne izmjene.

Upravljačko tijelo obvezno je osigurati razinu ulaganja u IKT i odrediti budžet koji je potreban kako bi se postigla visoka razina digitalne operativne otpornosti. Uzimajući u obzir temeljno načelo proporcionalnosti, može se zaključiti da je financijski subjekt kod određivanja odgovarajućeg budžeta obvezno u obzir uzeti veličinu, prirodu opseg i složenost usluga, aktivnosti i operacija financijskog subjekta.

U odnosu na Smjernice EIOPA-e o sigurnosti IKT [12] koje propisuju obvezu društva da prati razinu usklađenosti pružatelja usluga i postavlja određene zahtjeve za izdvajanje poslova u vezi s uslugama i sustavima IKT-a, Uredba DORA [8] izričito utvrđuje obvezu upravljačkog tijela da odobri i periodično preispita interne akte koji se odnose na ugovaranje usluga s trećim stranama pružateljima usluga IKT. Ujedno, financijski subjekti moraju osigurati proces urednog obavještavanja upravljačkog tijela o svim odnosima s trećim stranama i bitnim izmjenama, a osobito o potencijalnom učinku koji takvi odnosi imaju na ključne i važne funkcije.

Uredno obavještavanje upravljačkog tijela financijski subjekti moraju osigurati i u slučaju barem značajnih incidenata navodeći njihov učinak i mjere odgovora, oporavka i korektivne mjere.

Uredba DORA [8] uvodi i obvezu financijskih subjekata (izuzev mikropoduzeća) na uspostavu funkcije praćenja odnosa s trećim stranama pružateljima uslugama IKT. Uredba DORA [8] ostavlja na izbor financijskom subjektu između uspostave nove funkcije ili imenovanja člana višeg rukovodstva koji će biti odgovoran za nadzor rizika i prateće dokumentacije. Obzirom na navedeno, financijski subjekti svakako bi trebalo obrazložiti svoju konačnu odluku i uzeti u obzir potencijalni sukob interesa u slučaju imenovanja člana višeg rukovodstva kao i stručnost osobe kojoj će biti dodijeljena ova funkcija.

Osim što Uredba DORA [8] obvezuje upravljačko tijelo na podizanje svijesti o važnosti upravljanja rizicima IKT kao i edukaciju svog osoblja, upravljačko tijelo obvezno je redovito pohađati i posebna osposobljavanja. Ove edukacije trebale bi osigurati da upravljačko tijelo održava zadovoljavajuću razinu znanja i vještina u razumijevanju i procjeni rizika IKT i njihovom učinku na poslovanje financijskog subjekta. Budući da Uredba DORA [8] ne specificira u čijoj organizaciji bi se programi osposobljavanja upravljačkog tijela trebali

provoditi, za pretpostaviti je da bi se ovo trebalo odnositi barem na pohađanje programa osposobljavanja koje je financijski subjekt obvezan uspostaviti za svoje osoblje. Ipak, ova obveza svakako podiže ljestvicu upravljačkog tijela u upravljanju pažnjom dobrog gospodarstvenika odnosno pažnjom dobrog stručnjaka.

Iz gore navedenog vidljivo je da bi u odnosu na sustav upravljanja osiguravajuća društva već trebala imati uspostavljene procese upravljanja rizicima IKT koji u velikom dijelu odgovaraju zahtjevima Uredbe DORA [8]. U svrhu postizanja usklađenosti poslovanja osiguravajućeg društva s Uredbom DORA [8] osiguravajuće društvo mora utvrditi da li njihove aktivnosti ulaze u područje primjene Uredbe DORA [8], a što se osobito odnosi na posrednike u osiguranju i vanjsku prodajnu mrežu društva za osiguranje.

U svrhu ocjene rizika ugovaranja usluga s trećim stranama pružateljima usluga IKT, a osobito izdvajanja poslova ili funkcija, (re)osiguravajuća društva trebala bi utvrditi koji pružatelji usluga su obveznici primjene Direktive NIS-2 [3] i revidirati poslovne procese ocjene usklađenosti trećih strana s novim odredbama kao i potencijalni negativan učinak na poslovne procese (re)osiguravajućeg društva u slučaju neusklađenosti s novim odredbama.

Navedeno se osobito odnosi na ključne i važne subjekte pružatelje bankarskih usluga (kreditne institucije), pružatelje zdravstvene zaštite, digitalne infrastrukture (pružatelje usluga računarstva u oblaku, pružatelje usluga podatkovnog centra i pružatelju mreže za isporuku sadržaja), davatelje digitalnih usluga (pružatelji internetskih tržišta, internetskih tražilica i platforma za usluge društvenih mreža), pružatelje javnih elektroničkih komunikacijskih mreža, pružatelje usluga povjerenja, registre naziva vršnih domena i pružatelje usluga sustava naziva domena neovisno o veličini subjekta.

4.2. Upravljanje rizicima IKT

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 5-7 Uredbe DORA [8] *i Smjernicama EIOPA-e o sigurnosti IKT (smjernica broj 4)* [12]

Sukladno članku 5 Uredbe DORA [8] financijski subjekti obvezni su uspostaviti pisani okvir upravljanja rizicima IKT. Međutim, u planu implementacije potrebno je uzeti u obzir vrijeme i resurse koji će biti potrebni za usklađivanje alata, metoda, procesa i politika sukladno regulatornim tehničkim standardima koje su obvezne donijeti ESA. u suradnji s Agencijom Europske unije za kibersigurnost (dalje u tekstu: ENISA) unutar 12 mjeseci od stupanja na snagu Uredbe DORA. [8]

Sukladno članku 5 stavak 6 Uredbe DORA [8] financijske institucije obvezne su barem jednom godišnje i nakon svakog značajnog incidenta IKT ili povodom naloga nadzornog tijela provesti reviziju okvira upravljanja rizicima IKT. Opseg revizije i dokumentacija iste biti će utvrđena od strane ESA-e i ENISA-e.

Iako je isto nužna pretpostavka za uspostavu sustava upravljanja rizikom, Uredba DORA [8] jasno obvezuje financijski subjekt da identificira, klasificira i odgovarajuće dokumentira svoj informacijski sustav. Za razliku od Smjernica EIOPA-e o sigurnosti IKT [12] koja propisuje obvezu „mapiranja" informacijskog sustava, Uredba DORA [8] u članku 7 izričito propisuje popis elemenata koji moraju biti identificirani i registrirani kako slijedi: svi elementi sustava IKT, sve poslovne funkcije u području IKT, informacijska imovina, konfiguracija imovine i svih poslovnih procesa financijskog subjekta koji ovise o trećim stranama pružateljima usluga IKT. Dodatno, u članku 7 Uredba DORA [8] propisuje i obvezu procjene rizika IKT nad naslijeđenim sustavima jednom godišnje te prije i nakon povezivanja nove tehnologije, aplikacija ili sustava.

U odnosu na Smjernice EIOPA-e o sigurnosti IKT [12], uz kontinuirano praćenje i identifikaciju izvora rizika, Uredba DORA [8] zahtijeva identifikaciju i procjenu izloženosti riziku u odnosu na druge financijske subjekte. Nadalje, oba propisa predviđaju obvezne procjene rizika nakon svake velike promjene u infrastrukturi mrežnog i informacijskog sustava ili procesima ili informacijskoj imovini.

U uvodnoj izreci 39, Uredba DORA [8] upućuje na primjenu sustava, alata i tehnologija IKT u skladu s europskim i međunarodnim priznatim tehničkim normama ili najboljom sektorskom praksom. Članak 6 Uredbe DORA [8] propisuje uvjete koji moraju ispuniti sustavi, protokoli i alati financijskih institucija, međutim ovi uvjeti zapravo su smjernice financijskim subjektima budući da zadovoljavanje istih ovisi o samostalnoj procjeni svakog financijskog subjekta zasebno i to u određenom trenutku. Iz tog razloga izuzetno je važno da svaki financijski subjekt pisano argumentira primjerenost odabranih mjera tijekom odabira i nabave sustava, protokola i alata IKT i tijekom njihovog korištenja. Nadalje, sukladno Uredbi DORA [8] financijski subjekti trebali bi provoditi odgovarajuća testiranja kako bi mogli utvrditi pouzdanost, pravodobnost, dostatan kapacitet i preciznu obradu podataka kao i prognozirati najjače opterećenje nalozima, porukama ili transakcijama. Budući da sustavi, protokoli i alati moraju prema potrebi moći ispuniti dodatne potrebe za obradom informacija, financijski subjekti moraju predvidjeti moguće stresne okolnosti na tržištu ili druge nepovoljne situacije.

Implementacijski zahtjevi osiguravajućeg društva	Zahtjev i povezani zahtjevi
Identifikacija i uspostava/revizija registra svih poslovnih procesa zavisnih od funkcija IKT i njihova klasifikacija	1
Identifikacija poslovnih procesa koji ovise o trećim stranama pružateljima usluga IKT s naznakom na kritične funkcije	2
Identifikacija i uspostava/revizija registra imovine IKT koja podržava poslovne procese s naznakom imovine koja se nalazi na udaljenim lokacijama, klasifikacijom i vlasništvom	3
Identifikacija kritičnih i važnih funkcija i povezane imovine IKT	4
Mapiranje konfiguracije imovine i međuovisnost imovine IKT	5
Revizija rola i odgovornosti u upravljanju i korištenju servisa IKT sukladno povezanim poslovnim procesima	6
Identifikacija i uspostava/revizija registra rizika, ranjivosti i prijetnji IKT	7
Određivanje indikatora za redovno i izvanredno provođenje procjene rizika i uspostava poslovnog procesa i odgovornosti u provođenju procjene rizika	8
Određivanje indikatora i uspostava poslovnog procesa procjene rizika kod povezivanja naslijeđenog sustava i novih tehnologija, aplikacija ili sustava IKT	9
Određivanje vremenskog razdoblja periodičnog preispitivanja svih navedenih registara i indikatora za prepoznavanje velikih promjena u infrastrukturi mrežnog i informacijskog sustava, u procesima ili postupcima ili u informacijskoj imovini i povezane odgovornosti	10
Uspostava barem godišnjeg procesa procjene rizika naslijeđenih sustava IKT	11

Uspostava kontinuiranog praćenja rizika IKT i barem godišnjeg preispitivanja scenarija rizika	12
Uspostava/revizija poslovnog procesa nabave/razvoja sustava, alata i protokola IKT-a sukladno europskim ili međunarodnim normama	13
Utvrđivanje potrebnog kapaciteta za preciznu obradu podataka za pravodobno izvršavanje poslovnih procesa i pružanje usluga i povezano testiranje	14
Utvrđivanje razine najjačeg opterećenja nalozima, porukama i transakcijama	15

4.3. Zaštita, sprječavanje i otkrivanje incidenata

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 8-9 Uredbe DORA i [8] *Smjernicama EIOPA-e o sigurnosti IKT (smjernica broj 8,9,10,11,15)* [12]

Financijski subjekti obvezni su poduzimati mjere zaštite i sprječavanja nastanka incidenta IKT. Kako bi financijski subjekti predvidjeli mogući učinak rizika i odabrali odgovarajuće alate, politike i procedure za smanjenje učinka rizika sukladno članku 8 Uredbe DORA [8] nužan je kontinuiran nadzor i kontrola sigurnosti i funkcioniranja sustava IKT. Financijski subjekti obvezni su primijeniti načelo proporcionalnosti pri odabiru odgovarajućih rješenja i procesa koji će osigurati otpornost, kontinuitet i dostupnost sustava primjenom zaštitnih mjera u prijenosu podataka, u pohrani i korištenju podataka i u procesima upravljanja i administracije podacima. Usporedno sa Smjernicama EIOPA-e o sigurnosti IKT [12] , osiguravajuća društva već bi trebala imati uspostavljene mjere kojima se osigurava sigurnost operacija, upravljanje operacijama i upravljanje promjenama IKT.

Za uspješno upravljanje rizicima IKT ključno je brzo otkrivanje neželjenih aktivnosti. Sposobnost financijskog subjekta da brzo otkrije neželjenu aktivnost, uzrok problema s performansom mreže ili pojavu incidenata, izravno ukazuje na učinkovitost financijskog subjekta procjeni rizika koja se provodi temeljem povijesnih incidenata ili izmišljenih scenarija, na učinkovitost implementiranih kontrola preventivne i reaktivne zaštite i u konačnici na smanjenje potencijalnog negativnog učinka na poslovanje financijskog subjekta i treće osobe. U odnosu na otkrivanje, Smjernice EIOPA-e o sigurnosti IKT [12] propisuju obvezu

osiguravajućih društva na uspostavu kapaciteta za otkrivanje neuobičajenih aktivnosti i prijetnji što je u skladu i sa člankom 9 Uredbe DORA [8] koji obvezuje financijske institucije sukladno načelu proporcionalnosti na pravovremeno prepoznavanje neobičnih aktivnosti i bitnih jedinstvenih točki prekida.

Implementacijski zahtjevi osiguravajućeg društva	Zahtjev i povezani zahtjevi
Identifikacija prijetnji i ranjivosti podataka u prijenosu, pohrani, mirovanju i korištenju podataka i procjena rizika od gubitka integriteta, povjerljivosti i dostupnosti podataka, posebno u odnosu na kritične i važne funkcije	16 (7)
Revizija strategije, politike informacijske sigurnosti i drugih postupaka, protokola i alata kojima će se osiguravati otpornost, kontinuitet i dostupnost sustava IKT sukladno regulatornim tehničkim standardima koje će razviti ESA	17
Revizija politika, procedura i kontrola u vezi fizičke i logičke zaštite sukladno regulatornim tehničkim standardima koje će razviti ESA	18
Revizija mehanizama prepoznavanja, uspostave više razina kontrole i kriterija za otkrivanje i primjenu procesa odgovora na incidente IKT te mehanizme za automatsko obavještavanje sukladno regulatornim tehničkim standardima koje će razviti ESA	19
Uspostava/revizija poslovnog procesa upravljanja promjenama IKT i povezane odgovornosti osoblja u fazama testiranja, ocjene, odobravanja, implementacije i dokumentiranju procesa	20

4.4. Odgovori i oporavak, sigurnosne kopije i metode oporavka

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 10-13 Uredbe DORA [8] *i Smjernicama EIOPA-e o sigurnosti IKT (smjernica broj 14, 21,24)* [12]

U članku 10 Uredbe DORA [8] utvrđuje se obveza financijskih subjekata na donošenje politike kontinuiteta poslovanja s naglaskom na kritične i važne funkcije te usluge koje pružaju treće strane pružatelji usluga IKT, implementaciju planova odgovora i oporavka IKT i provođenje analize utjecaja na poslovanje primjenom kvantitativnih i kvalitativnih kriterija te na temelju internih i vanjskih podataka i analize scenarija. Navedeno je u skladu i sa Smjernicama EIOPA-e o sigurnosti IKT [12] stoga bi društvo za osiguranje već trebalo imati uspostavljene planove kontinuiteta poslovanja i odgovora i oporavka te provoditi analizu utjecaja na poslovanje. Uredba DORA [8] uvodi obvezu testiranja planova nakon svake značajne promjene sustava, ali obavezno barem jednom godišnje. Nadalje, Uredba DORA [8] obvezuje financijske subjekte na uspostavu funkcije za upravljanje kriznim situacijama i na obavještavanje nadležnih tijela o svim troškovima i gubicima uzrokovanim poremećajima u radu ili incidentima.

Implementacijski zahtjevi osiguravajućeg društva	**Zahtjev i povezani zahtjevi**
Revizija testiranja planova za kontinuitet poslovanja sukladno regulatornim tehničkim standardima koje će razviti ESA **Revizija planova odgovora i oporavka sukladno regulatornim tehničkim standardima koje će razviti ESA**	21
Za potrebe revizije osiguravajuće društvo trebalo bi provesti pripremne radnje:	
○ **identificirati ključne i važne funkcije osiguravajućeg društva, podržavajuće procese, ovisnost u odnosu s trećim stranama, podržavajuće informacijske alate i njihovu međuzavisnost**	22 (1,2,4,7,16)
○ **identificirati poslovne procese koji ovise o trećim stranama pružateljima usluga IKT s naznakom na kritične funkcije**	23 (2)
○ **raspisati različite scenarije incidenata i prilagođene mjere za ograničavanje štete i oporavka**	24

○ **uspostaviti metodologiju za procjenu učinka, procjenu štete i procjenu gubitaka povezanih s različitim vrstama incidenata**	25
○ **predvidjeti odgovorne osobe za upravljanje kriznim situacijama i tijek izvještavanja**	26
○ **utvrditi moguće incidente i revidirati planove oporavka prilagođene vrsti incidenta**	
○ **utvrditi kratkoročne i dugoročne mogućnosti oporavka**	27
○ **predvidjeti poslovni proces periodične revizije planova oporavka**	28
○ **predvidjeti poslovni proces testiranja barem jednom godišnje ili nakon svake velike promjene sustava**	29
Revidirati metode oporavka i vrstu podataka za koju se izrađuju sigurnosne kopije i učestalost izrade sukladno kritičnosti i povjerljivosti podataka i utvrditi razdoblje periodičnog testiranja	30
Revidirati mjere zaštite sustava IKT koji su fizički i logički odvojeni od glavnog sustava	31
Revidirati proces višestruke provjere cjelovitosti rekonstruiranih podataka	32
Revidirati dostatnost redundantnih kapaciteta IKT-a	33

4.5. Interna i vanjska komunikacija

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 12-13 Uredbe DORA [8] *i Smjernicama EIOPA-e o sigurnosti IKT (smjernica broj 15)* [12]

U skladu sa Smjernicama EIOPA-e o sigurnosti IKT [12] u članku 12 Uredbe DORA utvrđuje se obveza financijskog subjekta, izuzev mikropoduzeća, da provede analizu uzroka incidenta i moguća unaprjeđenja, međutim izričito navodi elemente koje takva analiza mora sadržavati i koji izvještaj mora biti pružen nadzornom tijelu na zahtjev.

Iako Smjernice EIOPA-e o sigurnosti IKT [12] već predviđaju obvezu osiguravajućeg društva na uspostavu programa osposobljavanja o informacijskoj sigurnosti za sve članove osoblja, sukladno članku 12 Uredbe DORA [8] utvrđuje se obveza financijskih institucija na razvoj

programa za podizanje svijesti za sve članove osoblja i upravljačkog tijela, ali prilagođene njihovoj odgovornosti i opisu radnog mjesta. Nadalje, iako se ne radi o novoj obvezi te nije utvrđena obveza dokumentiranja istog, u svrhu dokazivanja usklađenosti upravljanja rizicima, financijski subjekti trebali bi uspostaviti i dokumentirati proces praćenja tehnoloških dostignuća i najbolje prakse u upravljanju rizicima IKT te provoditi procjene učinka sigurnosnih mjera u svrhu transparentnog provođenja procesa ulaganja i nadogradnje sustava, sve sukladno načelu proporcionalnosti. Nadalje, sukladno članku 13 Uredbe DORA [8] financijski subjekti obvezni su uvesti komunikacijske planove incidenata što je također u skladu sa Smjernicama EIOPA-e o sigurnosti IKT [12]. Međutim kao novi zahtjev, nužno je imenovanje barem jedne osobe financijske institucije koja će u ovu svrhu biti zadužena za eksternu komunikaciju.

Implementacijski zahtjevi osiguravajućeg društva	Zahtjev i povezani zahtjevi
Revidirati poslovni proces analize incidenata i dokumentiranje iste uzimajući u obzir brzinu odgovora, razinu učinka incidenta, kvalitetu i brzinu obavljene forenzičke analize i učinkovitost interne eskalacije incidenta i unutarnje i vanjske komunikacije incidenta	34 (39)
Kod procjene rizika osiguravajućeg društva uzeti u obzir izvješća o provedenoj analizi	35 (8,9,11,16,25)
Uspostaviti proces mapiranja vremenske evolucije rizika	36 (8,9,11,16,25,)
Uspostaviti programe osposobljavanja prilagođene različitim razinama odgovornosti osoblja	37
Uspostaviti proces praćenja razvoja tehnologije	38 (12,24)
Revidirati poslovne procese i odgovornosti interne komunikacije i eskalacije incidenata i eksterne komunikacije incidenata s klijentima, dobavljačima, partnerima, nadzornim tijelima i javnosti	39 (34)

4.6. Upravljanje incidentima IKT

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 3, 15-17 Uredbe DORA [8] *i Smjernicama EIOPA -e o sigurnosti IKT (smjernica broj 15)* [12]

Kao što je ranije navedeno, u članku 3 Uredba DORA [8] razlikuje incident IKT kao „jedan ili više od strane financijskih institucija neplaniranih događaja koji ugrožavaju sigurnost mrežnih i informacijskih sustava i imaju negativan učinak na dostupnost, autentičnost, integritet ili povjerljivost podataka ili usluga koje pruža financijska institucija“ i značajan incident IKT kao „incident koji ima visoki negativan učinak na mrežni i informacijski sustav koji podupire kritične funkcije financijske institucije.“

Sukladno članku 3, Uredba DORA [8] preuzima definiciju kiberprijetnje iz Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (dalje u tekstu: Akt o kibersigurnosti) [17] i znači „svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno utjecati na mrežne i informacijske sustave, korisnike tih sustava i druge osobe.“

Dodatno, Uredba DORA [8] uvodi termin značajne kiberprijetne kao „kiberprijetnja čije tehničke karakteristike ukazuju da postoji potencijal nastanka značajnog incidenta IKT ili značajnog operativnog incidenta ili incidenta povezanog sa sigurnošću plaćanja.“

Smjernice EIOPA-e o sigurnosti IKT [12] također su predvidjele obvezu osiguravajućih društva da uspostave primjere kriterije i pragove za klasifikaciju događaja kao operativnog ili sigurnosnog incidenta, ali u skladu s kriterijima koje postavi društvo za osiguranje uzimajući u obzir kritičnosti usluge. Bez obzira na službene definicije Uredbe DORA [8], tumačenja i primjena navedenih definicija, odnosno klasifikacija incidenata unutar pojedinog financijskog subjekta, trebala bi se provoditi uzimajući u obzir njihov prioritet, ozbiljnost i kritičnost zahvaćene usluge sukladno regulatornim tehničkim zahtjevima kojima će ESA propisati kriterije i pragove značajnosti za utvrđivanje značajnih incidenata IKT i značajnih prijetnji IKT, a koje bi trebale biti izdane unutar 12 mjeseci od stupanja na snagu Uredbe DORA sukladno članku 16 [8].

Implementacijski zahtjevi osiguravajućeg društva	Zahtjevi i povezani zahtjevi
Revizija procedura za klasifikaciju incidenata i prijetnji sukladno regulatornim tehničkim standardima koje će razviti ESA	40
Uspostava poslovnog procesa analize, praćenja, evidentiranja incidenta i prikupljanja podataka u svrhu njegove kategorizacije i klasifikacije na način da se pravovremeno osigura prikupljanje podataka o: broju zahvaćenih korisnika ili financijskih partnera, trajanje i vrijeme prekida rada usluge, zahvaćeno zemljopisno područje i vrsta gubitka podataka, kritičnost zahvaćene usluge i neizravni i izravnu gubici i troškovi kao posljedica incidenta	41
Revizija registra svih incidenata uzimajući u obzir različitu klasifikaciju incidenta	42 (1,3,7)
Uspostava/revizija poslovnog procesa upravljanja incidentima s utvrđenim rolama i odgovornostima osoblja ovisno o vrsti incidenta	43
Uspostava procesa komunikacije značajnih incidenata upravljačkom tijelu	44 (7,16,40)

4.7. Prijava i izvještavanje o incidentima IKT i razmjena informacija o rizicima i incidentima IKT

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 17-20, 40Uuredbe DORA [8] *i Smjernicama EIOPA-e o sigurnosti IKT (smjernica broj 15)* [12] *i članka 26 Direktive NIS 2* [3].

Sukladno članku 17 Uredbe DORA [8] propisane su obveze financijskih subjekata na izvješćivanje relevantnog nadležnog tijela i klijenata ili korisnika usluga o značajnim incidentima i značajnim kiberprijatnjama ovisno o vrsti financijskog subjekta i ovisno o nadležnosti relevantnog tijela. Financijski subjekt obvezan je izvijestiti nadležno tijelo o značajnom incidentu IKT, kao i klijente odnosno korisnike ako isti imaju utjecaj na njihove

financijske interese, međutim izvješćivanje nadležnog tijela o značajnim prijetnjama IKT je dobrovoljno.

Budući da ESA u suradnji sa Zajedničkim odborom i ENISA-om i ESB-om u roku od 18 mjeseci od stupanja na snagu Uredbe DORA [8] tek moraju donijeti regulatorne tehničke standarde kojima će utvrditi sadržaj izvješća o značajnim incidentima IKT i sadržaj izvješća o značajnim kiberprijetnjama, utvrditi rokove u kojima je potrebno dostaviti početnu obavijest o incidentu i privremeno i završno izvješće, financijski subjekti moraju predvidjeti u implementacijskom planu vremenski prostor i resurse za daljnju razradu i implementaciju ovih poslovnih procesa. Proces izvješćivanja nadležnih tijela o značajnim incidentima IKT predviđen je na dvije razine. Prva razina u skladu s člankom 17 Uredbe DORA [8] odnosi se na razmjenu informacija o značajnim incidentima IKT između relevantnih nadležnih tijela koji su zaprimili početnu obavijest o incidentu i koji nakon primitka dostavljaju pojedinosti o incidentu ESA-i, ESB-u ako je isti nadležan, drugim relevantnim javnim tijelima, kao i nacionalnim nadležnim tijelima, jedinstvenoj kontakt točki ili CSIRT-u sve u skladu s Direktivom NIS-2 [3].

Drugu razinu izvješćivanja u skladu s člankom 17 Uredbe DORA [8] provode ESA i ESB koji uz savjetovanje s ENISA-om i u suradnji s relevantnim nadležnim tijelom razmatraju važnost značajnog incidenta IKT za druga relevantna tijela u drugim državama članicama nakon čega ih obavještavaju kako bi isti prema potrebi poduzeli sve potrebne mjere radi osiguravanja trenutne zaštite financijskog sustava.

Sukladno članku 19 Uredbe DORA [8], ESA bi u okviru Zajedničkog odbora uz savjetovanje ESB-a i ENISA-e u roku od 24 mjeseci od stupanja na snagu Uredbe DORA [8] trebale pripremiti izvješće s procjenom izvedivosti uspostave jedinstvenog EU čvorišta za izvješćivanje o značajnim incidentima IKT (*eng. EU Hub*). Sukladno uvodnoj izreci 43 Uredbe DORA [8] jedinstveno EU čvorište trebalo bi biti uspostavljeno ili u svrhu izravnog zaprimanja izvješća o značajnim incidentima IKT koje se prosljeđuje nacionalnim relevantnim tijelima, ili u svrhu centralnog mjesta pohrane zaprimljenih izvješća.

Budući da je sukladno članku 19 stavak 2 točka (e) Uredbe DORA [8] predviđeno pravo financijskih subjekata na pristup EU čvorištu, preostaje vidjeti tip modaliteta koje će utvrditi ESA-e kod uspostave čvorišta te što će to pravo pristupa praktično obuhvaćati. Uzimajući u obzir članak 20 stavak 2 Uredbe DORA [8] u skladu s kojim će ESA izdavati godišnja anonimizirana i agregirana izvješća o značajnim incidentima IKT (koja bi trebala služiti podrški

procjenama prijetnji i ranjivosti u području IKT-a), za pretpostaviti je da financijski subjekti neće imati uvid u anonimizirane pojedinačne prijavljene značajne incidente IKT putem jedinstvenog EU čvorištu nego će pristupom biti omogućena prijava značajnog incidenta IKT i praćenje statusa te eventualno pristup godišnjim anonimiziranim i agregiranim izvješćima.

Nadalje, sukladno članku 20 Uredbe DORA [8] nadležno tijelo trebalo bi nakon zaprimanja obavijesti i izvješća o incidentu, dostaviti financijskom subjektu povratnu informaciju ili okvirne smjernice u svrhu smanjenja negativnog učinka unutar financijskog sektora. Uzimajući u obzir da će ESA izdavati godišnja agregirana i anonimizirana izvješća o značajnim incidentima IKT, pretpostavka je da se ovakvim povratnim informacijama ili smjernicama pokušava harmonizirati način upravljanja incidentima IKT u financijskom sustavu. Međutim, sukladno članku 20 stavak 1 Uredbe DORA [8] nadležna tijela pružiti će povratnu informaciju samo u slučajevima kada je isto izvedivo, a što u ovom trenutku još ostaje nedorečeno.

Nadalje, neovisno o zaprimljenoj povratnoj informaciji, financijski subjekt ostaje u potpunosti odgovoran za upravljanje i posljedice prijavljenog incidenta IKT. Budući da iz navedenog proizlazi da nadležno tijelo pruža povratnu informaciju (*eng. feedback*), a ne obvezujuću uputu, te okvirne smjernice (*eng. high level guidance*), kao i da je financijski subjekt krajnje odgovoran za način upravljanja incidentom i njegove posljedice, iz istog proizlazi da navedene povratne informacije/smjernice nadležnog tijela neće biti obvezujuće za financijske subjekte.

Preostaje vidjeti kakav će biti odnos eventualnih neobvezujućih povratnih informacija nadležnih tijela koje zaprimaju financijski subjekti i tehničkih uputa, savjeta i mjera za rješavanje incidenta koja će izdavati nacionalni CSIRT-ovi sukladno članku 9. Direktive NIS [1]. Također, ostaje upitno hoće li ovakva vrsta međusektorskog izvješćivanja i pružanja uputa financijskim subjektima biti od stvarne pomoći pri upravljanju incidentima IKT, odnosno hoće li isto zaista dovesti do harmonizacije ili suprotno do nedosljednosti u upravljanju i proturječnosti u pruženim smjernicama.

Obzirom na krajnju odgovornost financijskog subjekta za upravljanje i posljedice prijavljenog značajnog incidenta IKT, financijski subjekti trebali bi imati predviđene mjere za upravljanje incidentima IKT prije nego se incident dogodi, odnosno redovno preispitivati učinkovitost mjera te ih prilagođavati najboljoj praksi, smjernicama, uputama nadležnih tijela i CSIRT-ova.

Konačno, budući da je člankom 17 stavak 4 Uredbe DORA [8] predviđena mogućnost da financijski subjekti u skladu s nacionalnim i sektorskim propisima, eksternaliziraju proces

izvješćivanja incidenata IKT trećoj strani, financijski subjekt trebao bi procijeniti rizik takve eksternalizacije uzimajući u obzir sektorske propise o izdvajanju poslova ili funkcija društva za osiguranje, a osobito uzimajući u obzir da je sukladno članku 17 Uredbe DORA [8] financijski subjekt krajnje odgovoran za izvršavanje obveze izvješćivanja.

U skladu s člankom 40 Uredbe DORA [8], financijski subjekti slobodni su odlučiti o razmjeni informacija u vezi kiberprijetnji, ugroženosti, taktikama i tehnikama, postupcima i upozorenjima te alatima s drugim financijskim subjektima. Cilj razmjene informacija trebao bi biti poboljšanje digitalne operativne otpornosti financijskog sektora te bi se takva razmjena trebala odvijati u pouzdanim zajednicama financijskih subjekata i u okviru zaštićenih mehanizama razmjena. Međutim, Uredba DORA [8] ne utvrđuje operativni okvir ovih razmjena. Usporedno, sukladno članku 26 Direktive NIS 2 [3], ključni i važni subjekti mogu međusobno razmjenjivati informacije o kiberprijetnjama, ranjivosti, pokazateljima ugroženosti, taktikama, tehnikama, upozorenjima i konfiguracijskim alatima. Budući da će sukladno članku 26. Direktive NIS 2 [3] ENISA poduprijeti uspostavu takvog mehanizma za razmjenu informacija i pružiti najbolje prakse i smjernice za razmjenu informacija, u ovom trenutku za pretpostaviti je da se i financijski subjekti kao obveznici primjene Uredbe DORA [8] mogu voditi istim smjernicama.

Implementacijski zahtjevi osiguravajućeg društva trebali bi uključivati:	**Zahtjevi i povezani zahtjevi**
Razmotriti mogućnost eksternalizacije procesa izvješćivanja sukladno regulatornim tehničkim standardima koje će razviti ESA	45
Uspostaviti proces izvješćivanja značajnih incidenata sukladno regulatornim tehničkim standardima koje će razviti ESA, u tri faze: 1. podnošenje početne obavijesti, 2. podnošenje privremenog izvješća onda kada dođe do značajne izmjene statusa incidenta ili su prikupljene informacije koje utječu na upravljanje incidentom i 3. podnošenje završnog izvješća nakon što se provede analiza incidenta i utvrdi temeljni uzrok i kada se utvrde stvarni podaci o učinku.	46

Identificirati scenarije za incidente koji potencijalno imaju učinak na financijske interese klijenata	47 (12,24)
Identificirati značajne kiberprijetnje i situacije u kojima postoji obveza informiranja klijenata o mjerama koje moraju poduzeti i uspostaviti proces izvješćivanja klijenata	48 (7,16,34,40)
Razmotriti učinkovitost uspostave procesa dobrovoljnog izvješćivanja značajnih kiberprijetnji	49 (17, 40, 42,44,46)

4.8. Upravljanje rizicima u odnosu s trećom stranom pružateljem usluga IKT

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 23-40 Uredbe DORA [8] *i Smjernicama EIOPA-e o sigurnosti IKT (smjernica broj 25)* [12] *te Smjernicama EIOPA-e o izdvajanju poslova pružateljima usluga računalstva u oblaku [18] te Smjernice EIOPA-e o sustavu upravljanja [19].*

Proces upravljanja izdvojenim poslovima ili funkcijama, društva za osiguranje trebaju provoditi sukladno odredbama Delegirane uredbe Komisije (EU) 2015/35 o dopuni Direktive 2009/138/EZ Europskog parlamenta i Vijeća o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja [20] i provedbenim pravilnicima, mišljenjima i preporukama nadležnih tijela.

Sukladno navedenom, izdvajanje ključnih ili važnih funkcija ne smije dovesti do značajnog pogoršanja kvalitete sustava upravljanja, neopravdano povećanog operativnog rizika, ugroze kontinuirane i zadovoljavajuće usluge ili smanjenja sposobnosti praćenja usklađenosti društva za osiguranje od strane nadzornih tijela. U slučaju izdvajanja poslova iz područja informacijskih i komunikacijskih tehnologija, uz navedene propise, potrebno je uzeti u obzir i voditi se Smjernicama EIOPA-e o sustavu upravljanja [19] i Smjernicama o izdvajanju poslova pružateljima usluga računarstva u oblaku [18].

Financijski subjekti koji sklapaju ugovore s trećim stranama pružateljima usluga IKT u potpunosti su odgovorni za usklađenost s primjenjivim propisima o financijskim uslugama sukladno članku 25 Uredbe DORA [8].

Financijski subjekti obvezni su uspostaviti okvir upravljanja i nadzora rizika koji proizlazi iz izdvajanja funkcija trećoj strani pružatelju usluga IKT te uključuje širok raspon trećih strana pružatelja usluga IKT, uključujući pružatelje usluga računarstva u oblaku, pružatelje softvera,

pružatelja usluga analize podataka, pružatelja usluga podatkovnog centra kao i pružatelje usluga plaćanja ili pružatelje operativne platne infrastrukture.

U smislu članka 25 Uredbe DORA [8] trećim stranama pružateljima usluga IKT smatraju se i one organizacije koje pružaju usluge drugim organizacijama unutar iste grupe poduzetnika.

4.8.1. Registar informacija i obavještavanje nadležnog tijela

Sukladno članku 25 Uredbe DORA [8] financijski subjekti obvezni su donijeti strategiju upravljanja rizikom u odnosu s trećim stranama pružateljima usluga IKT. U odnosu na Prijedlog DORA iz 2020. godine [6] u kojoj se navodi da strategija mora sadržavati politiku o korištenju usluga trećih strana pružatelja usluga IKT, Uredba DORA [8] mijenja zahtjev na način da ta strategija mora sadržavati politiku o ugovaranju treće strane pružatelja usluga IKT u odnosu na kritične i važne funkcije.

Nadalje, sukladno članku 25 Uredbe DORA [8] financijske institucije obvezne su uspostaviti i voditi registar informacija na konsolidiranoj i subkonsolidiranoj razini o svim ugovorima o korištenju usluga trećih strana pružatelja usluga IKT, a ne samo o onima koji se odnose na kritične i važne funkcije i usluge, ali s jasnim razlikovanjem te dvije kategorije.

Iako je registar svih izdvojenih usluga zapravo nužan u svrhu upravljanja rizicima, u odnosu na obveze društva za osiguranje, Smjernicama EIOPA-e o sigurnosti IKT [12] nije bila propisana formalna obveza vođenja registra svih izdvojenih funkcija i usluga.

Kao novi zahtjev u odnosu na dosadašnje obveze društava za osiguranje, uvodi se obveza financijskih subjekata da barem jednom godišnje obavještavaju nadležno tijelo o broju novih ugovora, vrsti ugovora, kategoriji treće strane pružatelja usluge IKT i vrsti usluge i funkcije koja se izdvaja. Nadalje, financijski subjekti obvezni su obavijestiti nadležno tijelo o planiranom ugovaranju, ali samo kritičnih ili važnih funkcija, ili izdvojenim funkcijama koje postanu kritične ili važne, što je u skladu i sa Smjernicama EIOPA-e o sigurnosti IKT [12]. Uredba DORA [8] ne navodi vremenski rok u kojem je potrebno poslati takvu obavijest nego koristi termin „pravodobno“ te ne navodi informacije koje takva obavijest mora sadržavati. Uzimajući u obzir gore navedeno, financijski subjekti biti će obvezni u barem dva navrata obavještavati nadzorno tijelo o izdvojenim kritičnim i važnim funkcijama, odnosno prije planiranog ugovaranja te u naknadnom izvješću koje se dostavlja nadležnim tijelima barem jednom godišnje. U odnosu na obveze društva za osiguranje u pogledu vremenskih rokova za dostavu obavijesti nadležnom tijelu o planiranom izdvajanju kritičnih ili važnih funkcija kao i

sadržaju takve obavijesti izgledno se i nadalje primjenjuju mjerodavne smjernice EIOPA-e [18], [19].

4.8.2. Primjerenost treće strane pružatelja usluga IKT

U odnosu na primjerenost treće strane pružatelja usluga IKT kojem se izdvajaju poslovi osiguravajućeg društva, među ostalim, Smjernice EIOPA-e o sigurnosti IKT [12] navode kako isti moraju ispunjavati odgovarajuće zahtjeve za korištenje usluga IKT ili sustava IKT. Nadalje, ako se izdvajaju kritične ili važne funkcije, treća strana pružatelj usluga IKT mora biti u mogućnosti provesti ugovorene odgovarajuće i proporcionalne ciljeve i mjere te minimalno ugovorene zahtjeve u pogledu informacijske sigurnosti, a s druge strane društva za osiguranje trebala bi tražiti jamstva u pogledu takve usklađenosti.

Usporedno, u članku 25 Uredba DORA [8] uvodi obvezu financijskih subjekata na ugovaranje suradnje isključivo s trećim stranama koje se pridržavaju odgovarajućih standarda informacijske sigurnosti. Dodatno, ako se izdvajaju ključne ili važne funkcije, financijski subjekti moraju uzeti u obzir one treće strane pružatelje usluga IKT koji zadovoljavaju visoke i najnovije standarde informacijske sigurnosti.

Uzevši u obzir da su financijski subjekti sukladno Uredbi DORA [8] i drugim sektorskim propisima u odabiru treće strane pružatelja usluga ograničeni određenim zahtjevima kao što su potencijalni sukob interesa i sposobnost pružatelja usluga na pridržavanje odgovarajućih standarda informacijske sigurnosti, odnosno najnovijih i najviših standarda informacijske sigurnosti, kao i sve druge čimbenike koje financijski subjekti uzimaju u obzir pri odabiru potencijalnog pružatelja, na konačan odabir pružatelja usluge i druge uvjete ugovaranja suradnje, svakako će utjecati dostupnost pružatelja usluga na tržištu koji su u mogućnosti ispuniti tražene zahtjeve.

Navedeno je usko povezano i s obvezom financijskog subjekta da prije sklapanja ugovora o korištenju treće strane pružatelja usluga IKT, uz procjenu svih relevantnih rizika, izvrše i preliminarnu procjenu koncentracijskog rizika temeljenu na analizi troškova i koristi, a do kojeg može doći u slučaju izdvajanja kritičnih ili važnih uslugu trećoj strani pružatelju usluga IKT koji nije lako zamjenjiv, ili financijska institucija s istim pružateljem ima više ugovora o pružanju usluga koje podržavaju kritične funkcije.

4.8.3. Provođenje nadzora i revizija treće strane pružatelja usluga IKT

Nadalje, iako je člankom 25 Uredbe DORA [8] propisano da financijski subjekti sukladno procjeni rizika utvrđuju učestalost i područje provođenja nadzora i revizije treće strane pružatelja usluga IKT, ovo nije izričito ograničeno na kritične i važne usluge. Međutim, budući da Uredba DORA [12] navodi kako se inspekcije i revizije provode sukladno uputama nadzornog tijela, za osiguravajuća društva inspekcije i revizije biti će obvezne za ključne i važne funkcije prema trenutno važećim smjernicama EIOPA-e [12].

U odnosu na Prijedlog DORA [6] kojom su bile utvrđene pretpostavke za obvezan raskid ugovora s trećom stranom pružateljem usluga IKT, Uredba DORA [8] utvrđuje minimalne uvjete pod kojima je moguće, ali nije ujedno i obveza, raskinuti ugovor s pružateljem usluga. Isto ujedno znači da će financijski subjekti morati provesti i dokumentirati analizu utjecaja na poslovanje i procjenu rizika u slučaju da jedan od navedenih uvjeta za raskid ugovora bude ispunjen kako bi u slučaju nadzora mogli argumentirati donesenu odluku o raskidu ili nastavku suradnje.

Pitanje učinkovitog nadzora i potencijalnog raskida ugovora postavlja se i kod preliminarne procjene koncentracijskog rizika gdje se propisuje obveza financijskog subjekta da izvrši procjenu hoće li potencijalni lanac podugovaratelja utjecati na mogućnost nadzornog tijela da učinkovito prati financijski subjekt. Naime, sukladno članku 31 Uredbe DORA [8] glavno nadzorno tijelo obvezno je dokumentirati i objasniti posljedice nemogućnosti provođena nadzornih aktivnosti pružatelja usluga koji se nalazi u trećoj zemlji o čemu je obvezno izvijestiti pružatelja usluga u sklopu preporuka koje izdaje temeljen provedenog nadzora, a osobito kada se preporuka odnosi na ispunjenje kumulativnih uvjeta temeljem kojih se preporuča suzdržavanje od sklapanja ugovora o podugovaranju usluge.

4.8.4. Sklapanje ugovora s trećom stranom pružateljem usluga IKT

U odnosu na sklapanje ugovora s trećom stranom pružateljem usluga IKT, u članku 27 Uredbe DORA [8] razlikuju se minimalne ugovorne odredbe koje moraju sadržavati svi ugovori i dodatne odredbe koje moraju sadržavati oni ugovori koji se odnose na izdvajanje ključnih ili važnih funkcija. Iako se navodi da bi prava i obveze ugovornih strana trebalo dokumentirati u jednom pisanom dokumentu, pretpostavka je da se ovo odnosi na svu relevantnu dokumentaciju koja bi trebala biti sastavni dio jednog krovnog ugovora.

Nadalje, iako je ugovorna odredba o obveznom ugovaranju izlazne strategije propisana isključivo za ugovaranje izdvajanja ključnih i važnih funkcija, općim odredbama koje se odnose

na sve ugovore uvodi se obveza ugovornih strana da ugovore odredbe kojima se osigurava pristup, oporavak i povratak svih podataka u slučaju raskida ugovora kao i drugi uvjeti raskida ugovora. Ovom odredbom zapravo se omogućilo financijskim subjektima i trećim stranama pružateljima usluga IKT da prilikom zaključenja ugovora primjene načelo proporcionalnosti.

Iako nije obvezno za svaki oblik suradnje s trećom stranom pružateljem usluga IKT, nego samo za izdvajanje ključnih i važnih funkcija, financijski subjekti trebali bi razmotriti ugovaranje izlazne strategije onda kada je isto svrsishodno obzirom da su u konačnici financijski subjekti u cijelosti odgovorni za osiguravanje digitalne otpornosti i osiguravanje kontinuiteta poslovanja. Ovdje treba uzeti u obzir da su financijski subjekti sukladno članku 28 Uredbe DORA [8] obvezni obavijestiti nadzorna tijela o situacijama kada funkcija ili usluga postane kritična ili važna stoga bi ugovorom koji sadrži samo opće zahtjeve uvijek trebalo predvidjeti i mogućnost izmjene ugovora sukladno zahtjevima koji su obvezni za izdvajanje ključnih ili važnih funkcija u slučaju da dođe do izmjene kategorizacije usluge za vrijeme trajanja ugovorene suradnje.

Nadalje, zanimljivo je da sukladno članku 27 Uredbe DORA [8] samo ugovori koji se odnose na ključne ili važne funkcije moraju sadržavati zahtjev da treća strana pružatelj usluge IKT uvede i testira planove za nepredvidive situacije u poslovanje te primjenjuje mjere i alate i politike za sigurnost IKT koji jamče financijskom subjektu sigurno pružanje usluga u skladu s regulatornim okvirom. Naime, sukladno članku 25 Uredbe DORA [8] koji postavlja opće zahtjeve u upravljanju rizicima trećih strana, financijski subjekti smiju zaključiti ugovore isključivo s onim trećim stranama pružateljima usluga IKT koji jamče i pruže dokaze o primjeni odgovarajućih standarda informacijske sigurnosti. Obzirom na navedeno, neovisno o tome izdvaja li se kritična i važna funkcija ili ne, treće strane pružatelji usluga IKT trebali bi imati uspostavljene planove za nepredvidive situacije te bi financijski subjekti, u skladu s načelom proporcionalnosti, trebali razmotriti dodavanje ove odredbe u sve ugovore.

Također, sukladno članku 27 Uredbe DORA [8] financijski subjekti obvezni su primjenom načela proporcionalnosti unaprijed utvrditi periodično provođenje nadzora i revizija. Međutim, sukladno članku 27 stavak 2 točka (e) Uredbe DORA [8] odredba o provođenju revizija i nadzora obvezna je samo za ugovore koji se odnose na ključne i važne funkcije. Naime, propisana je obveza ugovaranja odredbe prema kojoj financijski subjekti, ili imenovana treća strana i nadležno tijelo, imaju pravo kontinuiranog praćenja izvođenja usluge i neograničeno pravo na pristup, nadzor i reviziju koju provode.

S pravnog stajališta, za financijske subjekte rizik bi bio niži kada bi obveze pružatelja usluge bile utvrđene u Uredbi DORA [8] kako bi se izbjeglo netočno, različito ili dvosmisleno ugovaranje ovih odredbi, osobito jer se isto odnosi i na pravo pristupa, nadzora ili revizije od strane nadzornog tijela. Nadalje, istim stavkom propisuje se „kontinuirano praćenje“ i "neograničeno pravo pristupa, nadzora i revizije“ što je u koliziji s člankom 27 stavak 2 točka iii) Uredbe DORA [8] prema kojoj bi već u ugovoru trebalo utvrditi opseg, modalitete i učestalost nadzora i revizija.

Sukladno članku 12 stavak 6 Uredbe DORA [8], financijski subjekti obvezni su razviti programe dizanja svijesti o sigurnosti i digitalnoj otpornosti IKT koji su obvezujući za cijelo osoblje i upravljačko tijelo. Istom odredbom propisano je da će financijski subjekti, tamo gdje je primjenjivo, u programe dizanja svijesti i edukacije uključiti treće strane pružatelje usluga IKT. Međutim, člankom 27 Uredbe DORA [8] propisano je da će ugovori o pružanju usluge sadržavati uvjete pod kojima treće strane pružatelji usluga IKT sudjeluju u tim programima, dok bi učinkovitija bila odredba da su pružatelji usluga IKT obvezni sudjelovati u programima koje uspostavljaju financijski subjekti, osobito zato jer su drugi zahtjevi propisani upravo kao „obveze“ trećih strana pružatelja usluga IKT. Nesporno je da će se ugovorom utvrditi način i učestalost provođenja edukacija, ali ovakvim pravnim izričajem ostavlja se sloboda trećim stranama pružateljima usluga IKT na pregovaranje uvjeta sudjelovanja, dok je krajnja odgovornost za uspostavu i provedbu upravo na financijskim subjektima.

Konačno, člankom 27 stavak 3 Uredbe DORA [8] utvrđena je obveza financijskih subjekata i trećih strana pružatelja usluga IKT da razmotre korištenje standardnih ugovornih klauzula koje će razviti javne vlasti. Iz ovog proizlazi da financijski subjekti svakako moraju obrazložiti i dokumentirati svoju odluku u slučaju da se ne odluče na primjenu standardnih ugovornih klauzula. Budući da je krajnja odgovornost za usklađenost na financijskom subjektu, te da isključivo financijski subjekti imaju jedinstveni uvid u složenost funkcija i aktivnosti koje obavljaju, preporuka je da se standardne ugovorne klauzule uvijek koriste kao minimalne ugovorne odredbe, ali da se razmotre i drugi specifični rizici i prema potrebi dodatne odredbe radi osiguravanja višeg stupnja zaštite informacijskog sustava i osiguravanja digitalne operativne otpornosti.

4.8.5. Nadzorni okvir trećih strana pružatelju ključnih usluga IKT

4.8.5.1. Imenovanje trećih strana pružatelja ključnih usluga IKT

Nadalje, člancima 28-40 Uredbe DORA [8] propisan je nadzorni okvir za treće strane pružatelje ključnih usluga IKT sukladno kategorizaciji koju će provesti nadzorno tijelo. Međutim, nadzorni okvir imati će neizravan utjecaj i na financijske subjekte osobito u dijelu odabira pružatelja ključnih IKT usluga.

U okviru Zajedničkog odbora i na prijedlog nadzornog foruma, sukladno članku 28 stavak 1 a) Uredbe DORA [8], ESA će imenovati treće strane pružatelje ključnih usluga IKT. Odabir pružatelja ključnih usluga IKT provesti će se temeljem kriterija određenog člankom 28 stavak 2 Uredbe DORA [8] koji, među ostalim, uključuju i: „ukupan broj financijskih subjekata kojima pružatelj usluga pruža usluge, ukupnu vrijednost imovine financijskih subjekata, ovisnost financijskih subjekata na pružatelje usluga IKT u odnosu na ključne i važne funkcije i nepostojanje alternativnih pružatelja usluga IKT [8].

Naime, sukladno članku 28 stavak 7 Uredbe DORA [8] nadležna tijela jednom godišnje dostaviti će Nadzornom forumu anonimizirana i agregirana izvješća koja su prethodno zaprimili od financijskih subjekata s popisom novih ugovorenih usluga IKT, kategorijama pružatelja usluga, vrsti ugovornog odnosa i uslugama i funkcijama koje oni pružaju tim financijskim subjektima, a temeljem kojih će izgledno Nadzorni forum procijeniti ovisnost financijskih subjekata o uslugama trećih strana u svrhu određivanja pružatelja ključnih usluga IKT i uspostave nadzornog okvira.

Nadalje, kao što je ranije rečeno, prije ugovaranja usluge treće strane pružatelja usluga IKT, financijski subjekti dužni su provesti procjenu koncentracijskog rizika, a vidljivo je da će isti kriterij pratiti i Nadzorni forum pri utvrđivanju ovisnosti financijskih subjekata i alternativnih pružatelja usluga IKT. Iz navedenih odredbi proizlazi važnost financijskih subjekata u vođenju registra informacija i pravovremenom i potpunom izvještavanju nadzornih tijela i to radi harmonizacije kriterija za odabir pružatelja ključnih usluga IKT i uspostave harmoniziranog nadzornog okvira.

Uzimajući u obzir moguće posljedice za financijske subjekte zbog neusklađenosti trećih strana pružatelja usluga IKT s propisanim mjerama, za financijske subjekte od posebne je važnosti primanje informacija o statusu treće strane pružatelja usluga IKT u odnosu na nadzorni okvir koji se provodi nad trećim stranama pružateljima ključnih usluga IKT. Sukladno članku 28

stavak 2 točka (c) Uredbe DORA [8], treća strana pružatelj usluga IKT informirati će financijski subjekt kojem pruža usluge o činjenici da je imenovan kao pružatelj ključnih usluga IKT. Međutim, Uredba DORA [8] ne navodi rok u kojem treća strana pružatelj usluge IKT mora obavijestiti financijski subjekt, a što je od posebne važnosti budući da najkasnije u roku od 30 dana od kad pružatelj usluga IKT zaprimi informaciju o tome da je imenovan kao pružatelj ključnih usluga isti postaje podložan nadzornom okviru.

Uzimajući u obzir kriterije za određivanje ključnih i važnih funkcija financijskih subjekata i kriterije za odabir pružatelja ključnih IKT usluga, financijski subjekti trebali bi moći predvidjeti koje treće strane pružatelji usluga IKT će i formalno biti imenovani ključnima. Popis trećih strana pružatelja usluga IKT na razini Europske unije koji će jednom godišnje objavljivati ESA biti će od važnosti financijskim subjektima za planiranje strategije izdvajanja poslova i politike upravljanja ključnim i važnim funkcijama te procjenu povezanog rizika IKT svakog financijskog subjekta.

U tom smislu za financijske subjekte važna je i odredba članka 28 stavak 7 Uredba DORA [8] prema kojoj financijski subjekti mogu ugovoriti treću stranu pružatelja usluga IKT koja ima sjedište u trećoj zemlji isključivo pod uvjetom da je isti osnovao podružnicu u Europskoj uniji najkasnije 12 mjeseci otkad je imenovan kao ključan. Ovo je osobito važno za one treće strane pružatelje usluge IKT bez podružnice u Europskoj uniji koji se već nalaze u Registru informacija financijskih subjekata, ali i za sve buduće pružatelje usluga IKT. Naime, svi pružatelji usluga IKT koji se ne nalaze na listi pružatelja usluga koju godišnje objavljuje ESA mogu zatražiti pokretanje postupka imenovanja ključnima o čemu će konačnu odluku zaprimiti unutar 6 mjeseci od predaje zahtjeva. Obzirom na navedeno, financijski subjekti bi tijekom planiranja izdvajanja ključnih i važnih funkcija i odabira pružatelja usluga IKT, osobito onih koji nemaju sjedište niti podružnicu u Europskoj uniji, trebali uzeti u obzir određeno vremensko razdoblje za provedbu imenovanja i eventualne neizravne troškove vezane uz imenovanje pružatelja usluga IKT ključnim te bi svakako bilo oportuno ugovoriti uvjete za provedbu istog s trećom stranom pružateljem usluge IKT.

4.8.5.2. Nadzorni plan, preporuke nadzornog tijela i raskid ugovora

Nadalje, sukladno članku 28 stavak 1 točka (b) Uredbe DORA [8] ESA će imenovati Glavno nadzorno tijelo za svaku treću stranu pružatelja ključnih usluga IKT koji će provoditi nadzor pružatelja ključnih usluga IKT i koji će prvenstveno vršiti procjenu sustava za upravljanje rizicima IKT u odnosu na ključne i važne funkcije. Sukladno članku 30 stavak 2 Uredbe DORA

[8] ocjenjuje se ima li treća strana pružatelj usluga IKT uspostavljena djelotvorna i sveobuhvatna pravila, procedure, mehanizme i sustave upravljanja rizicima IKT relevantnim za financijske subjekte.

Glavno nadzorno tijelo će u suradnji sa Zajedničkom nadzornom mrežom i nakon usuglašavanja s trećom stranom pružateljem usluge IKT, donijeti Nadzorni plan koji će uključivati ciljeve godišnjeg plana nadzora i glavne radnje nadzora.

Za financijske subjekte od važnosti su preporuke koje izdaje Glavno nadzorno tijelo pružateljima usluga IKT sukladno članku 31 stavak 1 točka (d) Uredbe DORA [8]. Naime, Glavno nadzorno tijelo ovlašteno je izdavati preporuke pružateljima usluga IKT koje se odnose na primjenu konkretnih zahtjeva sa postizanje sigurnosti IKT kao što su zakrpe, ažuriranje i enkripcije, tehničku provedbu uvjeta kojima se sprječava nastajanje ili širenje jedinstvenih točaka prekida, preporuke za podugovaranje usluga ili za suzdržavanje od podugovaranja usluga. O identificiranim rizicima nadležno nadzorno tijelo obavijestiti će financijske subjekte budući da su sukladno članku 37 stavak 2 Uredbe DORA [8] financijski subjekti obvezni provoditi procjene rizika usluga izdvojenih trećim stranama.

Sukladno članku 31 stavak 4-9 Uredbe DORA [8], Glavno nadzorno tijelo ima ovlast izreći pružatelju usluga IKT periodičnu novčanu kaznu koja se izriče svakodnevno sve dok se ne osigura usklađenost pružatelja usluga IKT s propisanim preporukama ili u slučaju kada isto odbija dostaviti informacije i dokumentaciju potrebne za istragu ili nadzor, pa sve do najviše 6 mjeseci od dostave obavijesti o potrebnim mjerama. Iznos upravne novčane kazne računa se od datuma odluke kojom se izriče periodična kazna i jednak je 1 % prosječnog dnevnog svjetskog prometa treće strane pružatelja usluga IKT u prethodnoj poslovnoj godini.

Usporedno, sukladno članku 37 stavak 3 Uredbe DORA [8] kao posljednju mjeru nadležno nadzorno tijelo može zahtijevati od financijskog subjekta da privremeno obustavi, djelomično ili u cijelosti, izdvajanje usluga pružatelju usluga IKT sve dok se ne adresiraju rizici utvrđeni u preporukama Glavnog nadzornog tijela. Dodatno, tamo gdje je potrebno, nadležno nadzorno tijelo može zahtijevati od financijskih subjekata da raskinu, u cijelosti ili djelomično, ugovorne odnose s navedenim pružateljem usluga IKT.

Za financijske subjekte također je od važnosti činjenica da u slučaju da se treća strana pružatelj IKT usluga protivi izravnom nadzornu Glavnog nadzornog tijela, nadležna tijela financijskih subjekata mogu raskinuti ugovore sklopljene s pružateljem IKT usluga.

Obzirom na navedeno, razvidno je da je od neposredne važnosti svakog financijskog subjekta uložiti povećanu pažnju pri odabiru treće strane pružatelja usluga IKT kao i uspostaviti kontinuirani proces praćenja pružatelja usluga IKT i učinkovitu suradnju s istim osobito u razmatranju i provedbi preporuka dobivenih od nadležnih tijela u zadanim rokovima.

Treba napomenuti i da su financijski subjekti koji pružaju usluge IKT drugim financijskim subjektima i financijske institucije koje pružaju usluge IKT drugim financijskim subjektima unutar grupe poduzetnika isključeni iz nadzornog okvira za treće strane pružatelje ključnih IKT usluga.

Implementacijski zahtjevi osiguravajućeg društva	**Zahtjevi i povezani zahtjevi**
Uspostaviti Registar informacija o svim trećim stranama pružateljima usluga IKT sukladno regulatornim tehničkim standardima koje će razviti ESA, uzimajući u obzir posebne zahtjeve ključnih i važnih funkcija i usluga te pružatelje koji se nalaze u trećim zemljama	50 (1,2,3,4)
Izraditi/revidirati strategiju upravljanja rizicima pružatelja usluga i politiku o korištenju usluga trećih strana u odnosu na kritične i važne funkcije, uključujući:	51
○ **provjeru zakonskih uvjeta za izdvajanje funkcija ili usluga i sektorskih propisa od strane nadzornog tijela**	
○ **identifikaciju kritičnosti ili važnosti funkcije ili usluge koja se izdvaja i analizu utjecaja izdvajanja**	
○ **identifikaciju i analizu svih relevantnih rizika povezanih s izdvajanjem funkcije ili usluge**	
○ **analizu koncentracijskog rizika barem uzimajući u obzir analizu troškova i koristi, utjecaj podizvođača, propise o solventnosti i propise o zaštiti osobnih podataka**	
○ **provođenje dubinske analize potencijalne treće strane pružatelja usluga IKT uključujući kriterije za odabir**	

○ **ocjenu potencijalnog sukoba interesa s trećom stranom pružateljem usluga IKT**	
○ **reviziju metodologije ocjene primjene odgovarajućih standarda informacijske sigurnosti pružatelja usluge IKT**	
○ **reviziju metodologiju procjene rizika radi utvrđivanje učestalosti nadzora i revizije treće strane pružatelja usluga IKT**	
○ **reviziju izlaznih strategija i tranzicijskih planova koji moraju biti dokumentirani, testirani i periodično ažurirani**	
○ **analizu rizika podugovaranja usluge sukladno regulatornim tehničkim zahtjevima koje će razviti ESA**	
○ **strategiju praćenja nadzornog okvira pružatelja ključnih usluga IKT i utjecaja na poslovanje**	
Odrediti odgovorne osobu za vođenje i praćenje Registra informacija i izdvojenih funkcija i usluga i uspostaviti poslovni proces obavještavanja nadzornog tijela barem jednom godišnje i dodatno prije izdvajanja kritičnih ili važnih funkcija i usluga	51
Izraditi ugovorne klauzule s općim zahtjevima i s posebnim zahtjevima u odnosu na ključne i važne funkcije	52

4.9. Testiranje digitalne operativne otpornosti

Niža analiza odnosi se na pravne zahtjeve sukladno člancima 21-24 Uredbe DORA [8] *i Smjernicama EIOPA-e o sigurnosti IKT (smjernica broj 12)*

Sukladno uvodnim izrekama Uredbe DORA [8] testiranje digitalne operativne otpornosti uzduž financijskog sektora je vrlo segmentirano. Naime, pojedini podsektori financijskog sektora uspostavili su redovita testiranja sukladno sektorskim propisima i smjernicama, dok mnoge financijske institucije koje nisu obvezne provoditi testiranja iste niti ne provode što dovodi do povećanog rizika stabilnosti i integriteta cijelog financijskog tržišta.

Člankom 21 Uredbe DORA [8] utvrđuje se obveza financijskih subjekata, osim mikropoduzeća, da uspostave programe testiranja digitalne operativne otpornosti kao sastavni dio okvira upravljanja rizicima IKT u skladu s načelom proporcionalnosti. Upravo uz primjenu

načela proporcionalnosti, odnosno temeljem procjene rizika, financijski subjekti trebali bi utvrditi opseg sustava IKT koji će se testirati uzimajući u obzir razvoj rizika, ali i rizike ili druge čimbeniku koji su specifični za tu pojedinu financijsku instituciju. Iz ovog proizlazi važnost uspostave okvira upravljanja rizicima IKT koje će uključivati kontinuirani nadzor sigurnosti IKT unutar financijskog subjekta, ali i kontinuirano praćenje incidenata IKT unutar financijskog tržišta. Iako će opseg testiranja ovisiti o procjeni rizika financijskog subjekta, sukladno članku 21 Uredbe DORA [8] uvodi se obveza provođenja testiranja svih ključnih sustava i aplikacija barem jednom godišnje.

Testiranje ključnih sustava IKT jednom godišnje je i u skladu sa Smjernicama EIOPA-e o sigurnosti IKT prema kojima bi društva za osiguranje trebala provoditi testiranje kritičnih sustava IKT svake godine, stoga bi osiguravajuća društva već trebala imati uspostavljene poslovne procese testiranja otpornosti.

Primjena načela proporcionalnosti trebala bi omogućiti osiguravajućim društvima da za razliku od pojedinih drugih financijskih subjekata (za koje vrijede posebne odredbe Uredbe DORA [8]), u skladu s veličinom, prirodom, opsegom i složenosti usluga, te aktivnostima i operativnim radnjama koje provode, odnosno uslugama koje pružaju, imaju određenu slobodu u izradi programa testiranja i donošenju odluke o vrsti testova koje će se provesti.

Nadležna tijela utvrditi će koji financijski subjekti su obvezni barem jednom u tri godine, ali na zahtjev nadležnog tijela i češće, obvezni provesti napredno testiranje alata, sustava i procesa IKT-a na temelju penetracijskog testiranja vođenog prijetnjama nad nekoliko ili nad svim kritičnim ili važnim funkcijama i uslugama. Iako su kriteriji za odabir financijskih subjekata koji će morati provoditi napredno penetracijsko testiranje navedeni u članku 23 stavak 3 Uredbe DORA [8], za pretpostaviti je da će nadležna tijela biti u mogućnosti tumačiti obveznike primjene od slučaja do slučaja. Naime, sukladno Uredbi DORA [8] nadležno tijelo kod odabira uzima u obzir čimbenike povezane s učinkom i kritičnost usluge ili aktivnosti, učinak financijskog subjekta na nacionalnoj razini i na razini Europske unije i profil rizika konkretnog financijskog subjekta kao i zrelost financijskog subjekta da upravlja rizikom.

Harmonizacija u odabiru financijskih subjekata koje su obvezne provoditi penetracijsko testiranje očito bi se trebala postići primjenom nacrta regulatornih tehničkih standarda koje u roku od 18 mjeseci od dana stupanja na snagu Uredbe DORA [8] mora donijeti ESA i u kojima će među ostalim biti utvrđeni kriteriji, vrlo vjerojatno konkretniji od ovih koje navodi Uredba DORA[8].

Nadalje, iako članak 23 stavak 2 Uredbe DORA [8] propisuje da točan opseg penetracijskog testiranja vođenog prijetnjama utvrđuju financijski subjekti temeljem procjene rizika ključnih i važnih funkcija i usluga, i koji opseg potvrđuje nadležno tijelo, sukladno uvodnoj izreci 44 Uredbe DORA [8] financijski subjekti slobodni su utvrditi opseg testiranja samo u odnosu na to hoće li se sve ključne ili važne funkcije testirati u jednom penetracijskom testiranju ili u više njih. Dodatno, u sklopu nacrta regulatornih tehničkih standarda koje će donijeti ESA biti će utvrđeni i zahtjevi u odnosu na određivanje opsega testiranja.

Sukladno članku 21 stavak 5 Uredbe DORA [8] financijski subjekti obvezni su u potpunosti otkloniti sve slabosti, nedostatke i praznine koje će biti utvrđene s provedenim testiranjem iz čega proizlazi da isti moraju posvetiti osobitu pažnju kod određivanja opsega testiranja i korektivnih mjera obzirom da će se isto biti podložno i nadzoru nadležnih tijela. Naime, sukladno članku 23 Uredbe DORA [8] financijski subjekti na kraju penetracijskog testiranja i sastava izvješća, te dogovora oko planova sanacije, moraju dostaviti nadležnom tijelu sažetak nalaza, plan sanacije i dokumentaciju s kojom će dokazati da je penetracijsko testiranje provedeno u skladu sa svim zahtjevima u svrhu dobivanja potvrde o provedenom testiranju koja će biti prepoznata između različitih nadležnih tijela.

Nadalje, Smjernice EIOPA-e o sigurnosti IKT [12] propisuju da bi kod osiguravajućih društava testiranja trebala provoditi neovisni ispitivači koji imaju dovoljno znanja, vještina i stručnosti u testiranju mjera informacijske sigurnosti. U skladu s člankom 21 i 24 Uredbe DORA [8], testiranja, uključujući penetracijska testiranja, mogu provoditi unutarnji ili vanjski ispitivači i te je ključno osigurati njihovu potpunu neovisnost. Međutim, u odnosu na Smjernice EIOPA-e o sigurnosti IKT [12], članak 24 Uredbe DORA [8] utvrđuje stroge kriterije za odabir vanjskih pružatelja usluga penetracijskog testiranja koji kumulativno moraju biti ispunjeni.

Uzevši u obzir složenost pripremnih radnji koje je potrebno napraviti prije penetracijskog testiranja vođenog prijetnjama, analize nakon provedenog testiranja, kao i upitan broj što internih, a što vanjskih pružatelja usluga i ispitivača koji zadovoljavaju zahtjeve sukladno članku 24 Uredbe DORA [8], odnosno svih drugih potrebnih resursa, preostaje vidjeti hoće li financijski subjekti koji su obveznici provođenja ovog testiranja biti u mogućnosti provoditi ove zahtjeve. Naime, sukladno Smjernicama EIOPA-e o sigurnosti IKT [12], testiranje kritičnih sustava IKT-a i ispitivanje ranjivosti trebalo bi provoditi svake godine, ali opseg, učestalost i metode testiranja, uključujući penetracijska testiranja, društva za osiguranje trebala bi provoditi

razmjerno razini rizika koju sukladno načelu proporcionalnosti prvenstveno utvrđuje društvo za osiguranje.

Implementacijski zahtjevi osiguravajućeg društva	Zahtjevi i povezani zahtjevi
Uspostaviti program testiranja digitalne operativne otpornosti koji će sadržavati barem:	53
○ **identificirane ključne i važne funkcije osiguravajućeg društva i** • **podržavajuće procese, alate i njihovu međuzavisnost i aplikacije** • **funkcije i usluge koje su eksternalizirane ili ugovorene s trećim stranama pružateljima IKT usluga**	(1,2,3,4,50)
○ **odabrane metode testiranja alata i sustava sukladno načelo proporcionalnosti, uključujući provedbu procjena i skeniranja ranjivosti, analize otvorenih izvora, procjene mrežne sigurnosti, analize praznina, preispitivanja fizičke sigurnosti, upitnike i softverska rješenja za skeniranje, preispitivanja izvornog koda, testiranja na temelju scenarija, testiranje kompatibilnosti, testiranje radnih karakteristika**	1,2,3,4,5,6,7
○ **procedure za provedbu poslovnih procesa testiranja uključujući barem:** • **uloge i odgovornosti osoblja** • **proces utvrđivanja opsega testiranja i opsega penetracijskog testiranja sukladno regulatornim tehničkim standardima koje će razviti ESA** • **učestalost testiranja sukladno regulatornim tehničkim standardima koje će razviti ESA** • **proces odabira unutarnjih ili vanjskih ispitivača** • **metode testiranja** • **mjere zaštite podataka, servisa i ključnih funkcija za vrijeme testiranja**	55

• **utvrđivanje prioriteta problema uočenih tijekom testova, klasifikaciju i ispravke** • **metodologiju unutarnje provjere radi cjelovitog otklanjanja svih utvrđenih slabosti, nedostataka ili praznina.** • **Proces obavještavanja nadležnog tijela o utvrđenom opsegu testiranja i dostave izvješća i plana sanacije nadležnom tijelu**	

5. CERTIFIKACIJA PROIZVODA, USLUGA I PROCESA IKT

5.1. Mandat Agencije Europske unije za kibersigurnost sukladno novom regulatornom okviru

17. travnja 2019. donesen je Akt o kibersigurnosti [17] čiji cilj je osiguravanje mjera zaštite mrežnih i informacijskih sustava, telekomunikacijskih mreža, digitalnih proizvoda, usluga i uređaja.

Aktom o kibersigurnosti [17] mjere zaštite od kiberprijetnji usmjerene su na uspostavu osnovnih pravila kiberhigijene čiji cilj je integrirana sigurnost proizvoda IKT, usluga IKT i procesa IKT malih, srednjih i velikih poduzeća te operatora ključnih infrastruktura, što bi u konačnici trebalo podići osviještenost i povjerenje potrošača u doba rasta razvoja digitalizacije, a osobito u slučaju međusobne povezanosti komponenata i tehnologija proizvoda, usluga i procesa IKT jedne organizacije s komponentama trećih strana.

Sukladno Aktu o kibersigurnosti [17] poduzeća, organizacije i javni sektor trebale bi zadanom konfiguracijom proizvoda, usluga i procesa omogućiti krajnjim korisnicima najvišu razinu sigurnosti. Aktom o kibersigurnosti mijenja se mandat ENISA-e radi postizanja njene veće djelotvornosti u kontekstu razvoja kibersigurnosti i porasta različitih vrsta kiberizazova.

Osnovni cilj ENISA-e i nadalje uključuje njenu ulogu kao glavne točke za savjetovanje Europske komisije, država članica, javnih tijela i privatnih poduzeća, pružanje stručnog znanja i posredovanje. Međutim, u svrhu povećanja njene djelotvornosti, ENISA koja se osniva Aktom o kibersigurnosti [17] nasljeđuje ENISA-u osnovanu Uredbom (EU) br. 526/2013 [21] te

uključuje i promicanje najbolje prakse, davanje prijedloga o regulatornim i sektorskim aktima i provođenje operativne suradnje između država članica i ostalih dionika te izvršavanje zadaća dodijeljenih joj drugim pravnim aktima. Ovo se prvenstveno odnosi na osiguravanje dosljedne provedbe Direktive NIS 2 [3] prema kojoj se proširuje područje djelovanja ENISA-e.

U skladu s navedenim, sukladno članku 5 stavak 4 Direktive NIS 2 [3] na zahtjev države članice, ENISA će istima pomoći u razvoju nacionalne strategije za kibersigurnost. Nadalje, sukladno članku 6 stavak 2 Direktive NIS 2 [3], ENISA uspostavlja europski registar ranjivosti koji će uključivati informacije o ranjivosti, ozbiljnost ranjivosti i smjernice za ublažavanje rizika, a sukladno članku 9 Direktive NIS 2 [3] na zahtjev države članice, pružiti će pomoć u razvijanju nacionalnih timova za odgovor na računalne sigurnosne incidente (*eng. CSIRT*). ENISA uspostavlja i registar subjekata koji pružaju prekogranične usluge te ove informacije prosljeđuje jedinstvenim kontakt točkama sukladno članku 25 Direktive NIS 2 [3].

Sukladno članku 12 stavak 3 Direktive NIS2 [3] predstavnik ENISA-e sudjelovati će u aktivnostima skupine za suradnju radi olakšavanja suradnje i razmjene informacija između država članica Europske unije s europskim nadzornim tijelima što je također u skladu s relevantnim odredbama Uredbe DORA [8],

ENISA će ujedno osigurati tajništvo i podržati suradnju između timova nadležnih za odgovor na sigurnosne incidente kao i tajništvo i razmjenu informacija između Europske mreže organizacija za vezu za kiberkrize (*eng. EU-CyCLONe*) uspostavljene radi koordinacije upravljanja kiberincidentima velikih razmjera sukladno članku 13 i Direktive NIS-2 [3] te organizirati prikladne vježbe u području kibersigurnosti.

Nadalje, zadaća ENISA-e ujedno je izdavanje dvogodišnjih izvješća o stanju kibersigurnosti u Europskoj uniji te relevantnih preporuka za povećanje kibersigurnosti koje izdaje u suradnji s Europskom Komisijom sukladno članku 13 Direktive NIS 2 [3].

U suradnji s Europskom Komisijom i Skupinom za suradnju, ENISA savjetuje i tijekom utvrđivanja metodologije i sadržaja istorazinskog ocjenjivanja kojim će se provoditi ocjena učinkovitosti politika država članica u području kibersigurnosti te će imenovati stručnjake promatrače sukladno članku 16 Direktive NIS 2 [3] te provoditi koordinirane procjene sigurnosnih rizika za ključne lance opskrbe proizvoda, usluga i procesa IKT. U slučaju incidenata koji imaju znatan učinak na pružanje usluga ključnih i važnih subjekata i koji pogađaju dvije ili više država članica, ENISA će prema potrebi zaprimiti obavijest od

nadležnog tijela države članice ili nadležnog tima za upravljanje sigurnosnim računalnim incidentima, kao i mjesečno izvješće o incidentima, ozbiljnim prijetnjama i izbjegnutim incidentima od jedinstvene kontaktne točke sve u skladu s člankom 19 Direktive NIS 2 [3].

Budući da sukladno članku 26 Direktive NIS 2 [3] ključni i važni subjekti mogu međusobno razmjenjivati informacije o kiberprijetnjama, ranjivosti, pokazateljima ugroženosti, taktikama, tehnikama, upozorenjima i konfiguracijskim alatima, ENISA će poduprijeti uspostavu takvog mehanizma za razmjenu informacija pružanjem najbolje prakse i smjernica.

Budući da je Uredba DORA [8] u odnosu na Direktivu NIS 2 [3] *lex specialis* u odnosu na financijski sektor, jasno je da je njome utvrđeno široko područje djelovanja ENISA-e. Naime, sukladno članku 14 Uredbe DORA [8] ESA će u suradnji s ENISA-om izraditi nacrt regulatornih tehničkih standarda u svrhu utvrđivanja sljedećeg: mjera za osiguranje sigurnosti mreža; mjera zaštite od neovlaštenih upada i zlouporabe podataka, očuvanje autentičnosti i cjelovitosti; kriptografske tehnike; mjere za točan i brz prijenos podataka; odgovarajuće tehnike, metode i protokole za integriranu sigurnost; automatizirane mehanizme izoliranja zahvaćene informacijske imovine u slučaju kibernapada; kontrole o opozivu prava pristupa; mjere za otkrivanje incidenata; smjernice za izradu plana oporavka i politike kontinuiteta poslovanja te relevantne scenarije za njihovo testiranje.

Nadalje, sukladno članku 16 i 18 Uredbe DORA [8], ENISA će savjetovati ESA-u i Zajednički odbor u donošenju kriterija za utvrđivanje značajnih rizika IKT i odrediti će sadržaj izvješća o incidentu koji moraju predati financijski subjekti.

Usporedno s Direktivom NIS 2 [3] prema kojoj ENISA vodi registar kiberranjivosti, sukladno članku 19 Uredbe DORA [3] ESA i Zajednički odbor će u suradnji s ENISA-om procijeniti izvedivost daljnje centralizacije izvješćivanja o značajnim incidentima IKT uvođenjem jedinstvenog EU čvorišta za izvješćivanje.

5.2. Europski programi kibersigurnosne certifikacije

U svrhu dokazivanja usklađenosti ključnih i važnih subjekata s određenim razmjernim tehničkim i organizacijskim mjerama upravljanja rizicima, sukladno članku 21 Direktive NIS 2 [3] i članku 56 Akta o kibersigurnosti [17] države članice mogu zahtijevati da ključni i važni subjekti certificiraju određene proizvode, usluge i procese IKT u okviru posebnih europskih programa kibersigurnosne certifikacije.

Naime, sukladno članku 48 Akta o kibersigurnosti [17], Europska komisija može zatražiti od ENISA-e da izradi prijedlog programa certifikacije ili da preispita postojeći.

Programom kibersigurnosne certifikacije utvrđuje se osnovna, znatna ili visoku razina zaštite, razmjerno razini rizika koji se odnosi na proizvod, proces ili uslugu IKT te se određena jamstvena razina navodi u europskom kibersigurnosnom cerrtifikatu i EU izjavama o sukladnosti.

Sukladno članku 52 stavak 5 Akta o kibersigurnosti [17] osnovna jamstvena razina uključuje „jamstvo da proizvodi, usluge i procesi IKT za koje su taj certifikat ili ta EU izjava o sukladnosti izdani, ispunjavaju odgovarajuće sigurnosne zahtjeve, uključujući sigurnosne funkcionalnosti, te da su bili podvrgnuti evaluaciji na razini čija je svrha svođenje na najmanju moguću mjeru poznatih osnovnih rizika za incidente i kibernapade. Aktivnosti evaluacije koje treba poduzeti obuhvaćaju barem preispitivanje tehničke dokumentacije. Ako takvo preispitivanje nije odgovarajuće, poduzimaju se zamjenske aktivnosti evaluacije s istovjetnim učinkom.“ [17]

U odnosu na znatnu razinu, „znatna razina zaštite predviđa evaluacije na razini čija je svrha svođenje na najmanju moguću mjeru poznatih kibersigurnosnih rizika te rizika od incidenata i kibernapada koje provode subjekti ograničenih vještina i resursa. Aktivnosti evaluacije koje treba poduzeti obuhvaćaju barem sljedeće: preispitivanje radi dokazivanja nepostojanja javno poznatih ranjivosti i testiranje radi dokazivanja da proizvodi, usluge ili procesi IKT na ispravan način primjenjuju potrebne sigurnosne funkcionalnosti. Ako bilo koja od tih aktivnosti evaluacije nije odgovarajuća, poduzimaju se zamjenske aktivnosti evaluacije s istovjetnim učinkom.“ [17]

Konačno, visokom razinom zaštite „pruža se jamstvo podvrgnute evaluacije na razini čija je svrha svođenje na najmanju moguću mjeru rizika od najsuvremenijih kibernapada koje provode subjekti znatnih vještina i resursa. Aktivnosti evaluacije koje treba poduzeti obuhvaća barem sljedeće: preispitivanje radi dokazivanja nepostojanja javno poznatih ranjivosti; testiranje radi dokazivanja da proizvodi, usluge ili procesi IKT na ispravan način i na najsuvremenijoj razini primjenjuju potrebne sigurnosne funkcionalnosti; procjenu njihove otpornosti na napad vještih napadača, koristeći se penetracijskim testiranjem. Ako bilo koja od tih aktivnosti evaluacije nije odgovarajuća, poduzimaju se zamjenske aktivnosti s istovjetnim učinkom.“ [17]

Svaki program kibersigurnosne certifikacije mora sadržavati barem sljedeće ciljeve sukladno članku 51 Akta o kibersigurnosti [17]:

- „zaštitu pohranjenih, poslanih ili na drugačiji način obrađenih podataka od slučajnog ili neovlaštenog pohranjivanja, obrade, pristupa ili objave tijekom cijelog životnog ciklusa proizvoda, usluga ili procesa IKT;
- zaštitu pohranjenih, poslanih ili na drugačiji način obrađenih podataka od slučajnog ili neovlaštenog uništavanja, gubitka ili izmjene ili nedostatka dostupnosti tijekom cijelog životnog ciklusa proizvoda, usluge ili procesa IKT;
- da ovlaštene osobe, programi ili strojevi mogu pristupiti isključivo podacima, uslugama ili funkcijama na koje se odnose njihova prava pristupa;
- utvrđivanje i dokumentacija poznatih ovisnosti i ranjivosti;
- evidentiranje kojim se podacima, uslugama ili funkcijama pristupilo i koji su podaci, usluge ili funkcije upotrijebljeni ili na drugi način obrađeni, kada i tko je to učinio;
- mogućnost provjere kojim se podacima, uslugama ili funkcijama pristupilo i koji su podaci, usluge ili funkcije upotrijebljeni ili na drugi način obrađeni, kada i tko je to učinio;
- mogućnost provjere da li proizvodi, usluge i procesi IKT ne sadrže poznate ranjivosti;
- pravodobno osiguravanje ponovne dostupnosti podataka i pristup podacima, uslugama i funkcijama u slučaju fizičkog ili tehničkog incidenta;
- da su proizvodi, usluge i procesi IKT zadanim postavkama i dizajnom sigurni;
- da proizvodi, usluge i procesi IKT imaju osiguran ažuriran softver i hardver koji ne sadrže javno poznate ranjivosti te imaju osigurane mehanizme za sigurno ažuriranje.“

Kako navodi Akt o kibersigurnosti [17], svrha Europskog okvira za kibersigurnosnu certifikaciju je povećanje razine kibersigurnosti u Europskoj uniji i harmoniziran pristup za europske programe kibersigurnosne certifikacije kojim bi se trebalo postići jedinstvenost digitalnog tržišta u području proizvoda, usluga i procesa IKT. Uzimajući u obzir gore navedene sigurnosne zahtjeve za ključne i važne subjekte sukladno Direktivi NIS 2 [3], zatim sigurnosne zahtjeve za postizanje digitalne operativne otpornosti financijskih subjekata sukladno Uredbi DORA [8], široko i sveobuhvatno područje djelovanje ENISA-e prema različitim propisima, te planirane provedbe nadzora ključnih, važnih, financijskih subjekata i trećih strana pružatelja usluga, neovisno o moguće nužnoj certifikaciji određenih subjekata utvrđenoj od strane država članica, ključni i važni subjekti, a osobito financijski subjekti, svakako bi trebali pratiti programe certifikacije u izradi, potencirati izradu sektorskih programa, te razmotriti

certificiranje vlastitih usluga, proizvoda i procesa IKT ovisno o procijenjenoj razini rizika. Naime, upravo dobivanje Europskog sigurnosnog certifikata može biti od pomoći ključnim i važnim subjektima, odnosno financijskim subjektima, u demonstraciji usklađenosti sa sigurnosnim zahtjevima mjerodavnih propisa pri provođenju nadzora od strane nadležnih tijela, kao i u postizanju jačanja povjerenja krajnjih korisnika, odnosno potrošača u sigurnost proizvoda, usluga i procesa IKT kao i u stabilnost financijskog sustava.

6. IZDVAJANJE POSLOVA PRUŽATELJIMA USLUGA RAČUNARSTVA U OBLAKU

Uzimajući u obzir propise navedene u ranijim poglavljima, niže se navodi primjer obveza društva za osiguranje u slučaju izdvajanja poslova pružateljima usluga računarstva u oblaku. Društva za osiguranje uzeti će u obzir sektorske propise koji su u većini zahtjeva usklađeni s odredbama Uredbe DORA [8].

Prije ugovaranja suradnje s trećom stranom pružateljem usluga, sukladno Smjernicama EIOPA-e o izdvajanju poslova pružateljima usluga računarstva u oblaku [18] društvo za osiguranje obvezno je sukladno načelu proporcionalnosti izvršiti:

- provjeru smatra li se predmetna usluga izdvajanjem poslova u smislu Direktive o Solventnosti II [10];
- provjeru odnosi li se izdvajanje na pružanje usluge računarstva u oblaku ili se pružatelj usluga oslanja na infrastrukturu računarstva u oblaku tijekom pružanja svojih usluga;
- provjeru usklađenosti planiranog izdvajanja s internim aktima o izdvajanju poslova;
- ažurirati evidenciju sporazuma o izdvajanju poslova;
- procjenu rizika s korištenjem usluga u oblaku ovisno o odabranom modelu i ovisno o podacima i uslugama koje se izdvajaju (procjenu rizika povezanih s rizicima IKT-a i migracije podataka, procjenu operativnih rizika, procjenu rizika kontinuiteta poslovanja, procjenu pravnih rizika, procjenu reputacijskih rizika i koncentracijskog rizika);
- procjenu odnosi li se izdvajanje poslova na ključne i važne funkcije;
- provesti dubinsku analizu i ocjenu primjerenosti treće strane pružatelja usluga;
- provjeriti mogući sukob interesa s pružateljem usluga;

U postupku odabira treće strane pružatelja usluga osiguravajuća društva moraju utvrditi je li pružatelj usluga u mogućnosti zadovoljiti kriterije koji će biti propisani pisanom strategijom i pravilima osiguravajućeg društva o izdvajanju poslova. Sukladno Smjernicama EIOPA-e o

izdvajanju poslova pružateljima usluga računarstva u oblaku [18] društvo za osiguranje obvezno je provesti dubinsku analizu pružatelja usluge neovisno o vrsti poslova koja se izdvajaju i osigurati da se pružatelji usluga pridržavaju relevantnih propisa i odgovarajućih standarda iz područja informacijske i komunikacijske tehnologije. U slučaju izdvajanja ključnih ili važnih poslova uz dubinsku analizu potrebno je provesti i ocjenu primjerenosti pružatelja usluga.

U slučaju izdvajanja ključnih ili važnih usluga društvo za osiguranje i pružatelj usluga moraju zajednički usuglasiti sljedeće zahtjeve [18]:

- uloge i odgovornosti na način da iste budu jasno razdvojene;
- primjerenu razinu zaštite povjerljivosti, cjelovitosti i sljedivosti podataka;
- mjere zaštite podataka u prijenosu, pohranjenih podataka i neaktivnih podataka;
- mjere osiguravanja kontinuiteta poslovanja, dostupnosti podataka i usluge i očekivani kapacitet mrežnog prometa;
- integraciju usluga računalstva u informacijski sustav društva;
- postupak upravljanja korisnicima i pravima pristupa;
- postupak i odgovornosti u upravljanju incidentima IKT;
- lokaciju pohrane i obrade podataka;
- mjere kontrole i nadzora ispunjavanja utvrđenih zahtjeva i učinkovitosti.

Uzimajući u obzir gore navedene propise, društvo za osiguranje u ocjeni primjerenosti treće strane pružatelja usluga računarstva u oblaku, trebalo bi uzeti u obzir i sljedeće:

- posjeduje li pružatelj usluga certifikat ISO 27001 ili drugi međunarodno priznati certifikat;
- provjeru javno dostupnih povijesnih podataka o sigurnosnim incidentima, a osobito incidentima koji uključuju povrede osobnih podataka;
- lokaciju obrade podataka (u prijenosu i pohranjenih podataka). Obzirom da društva za osiguranje u pravilu raspolažu s osobnim podacima klijenata, u svrhu osiguravanja visoke razine zaštite obrada podataka trebala bi se provoditi na području Europske unije;
- ima li pružatelj usluga uspostavljene procese praćenja ranjivosti i prijetnji i strategiju upravljanja rizikom IKT;
- metode odgovora i oporavka pružatelja usluge, mogućnost generiranja log zapisa i pravila i rokove za provođenje analize u slučaju incidenata;
- provodi li pružatelj usluga redovita testiranje digitalne operativne otpornosti;

- omogućuje li pružatelj usluga enkripciju podataka u prijenosu i mirovanju;
- omogućuje li pružatelj usluga upravljanje identitetom i pristupom prema modelu temeljenom na ulogama i sukladno načelu najmanjih privilegija te višefaktorsku autentifikaciju;
- ograničenja prava pristupa podacima od strane pružatelja usluga;
- ograničenja i rizike povezane s podugovaranjem usluge;
- mjere za osiguravanje sigurnosti krajnjih točaka;
- postoje li uspostavljeni procesi redovitog praćenja i usklađenosti pružanja usluge s propisima o u području zaštite podataka i informacijskom sigurnosti u poslovnim procesima pružatelja usluga i sposobnost pružatelja usluga za postupanje u nepredvidivim situacijama;
- omogućuje li pružatelj usluga edukaciju korisnika i različite razine tehničke podrške;
- omogućuje li pružatelj usluga društvu za osiguranje redoviti nadzor, praćenje izvođenja usluge i revizije,
- odgovornosti i ulogu pružatelja usluge te njegovu mogućnost ispunjenja obveza u provođenju izlazne strategije, migracije podataka, dostupnosti usluge i brisanja podataka.

7. ZAKLJUČAK

Uredba DORA [8] prvi je zakonodavni akt kojim se na razini Europske unije donose sveobuhvatna pravila za postizanje digitalne operativne otpornosti za većinu subjekata financijskog sektora. Uzimajući u obzir postojeće regulatorne okvire sektorskih propisa kao i smjernice različitih nadzornih tijela, Uredba DORA [8] u velikom dijelu replicira već postojeće sektorske zahtjeve za postizanje kibersigurnosti i učinkovito upravljanje u području informacijskih i komunikacijskih tehnologija.

Uredba DORA [8] usklađuje poslovne strategije financijskih subjekata i nesporno utvrđuje potpunu odgovornost upravljačkog tijela u upravljanju rizicima informacijsko komunikacijskih tehnologija. U održavanju kiberhigijene informacijskih sustava, financijski subjekti obvezni su primijeniti osnovno načelo proporcionalnosti i prilagoditi tehničke i organizacijske mjere u skladu s generalnim profilom rizika kompanije uzimajući u obzir prirodu, opseg i složenost usluga, aktivnosti i operativnih radnji koje provode u pružanju financijskih usluga. Primjena načela proporcionalnosti će u svakom slučaju i nadalje voditi određenom odstupanju od harmonizirane primjene pravila za postizanje visoke razine digitalne operativne otpornosti. Načelo primjene proporcionalnosti djelomično se ograničava uspostavom nadzornog okvira i utvrđivanjem trećih strana pružatelja ključnih usluga od strane nadležnih tijela.

Okvir upravljanja rizicima IKT financijskih subjekata barem mora uključivati kontinuiranu analizu rizika informacijskih sustava, učinkovite sigurnosne mjere za sprječavanje i otkrivanje incidenata i mjere za upravljanje rizikom kojima će se ograničiti mogući nastanak štete nakon kibernapada.

Financijski subjekti obvezni su uspostaviti strategije, politike i provedbene procedure radi dodjele uloga i odgovornosti osoblja koje upravlja i koristi sustave IKT, kao i planove za provođenje periodičnog testiranja digitalne operativne otpornosti te planove oporavka odgovora i kontinuiteta poslovanja.

U svrhu razmjene informacija o incidentima IKT na razini država članica i Europske unije, financijski subjekti obvezni su uspostaviti poslovne procese radi brzog otkrivanja i izvješćivanja nadležnih tijela o incidentima IKT i kontinuirano praćenje i evidentiranje incidenata IKT i povezanih kiberprijetnji.

Obveznim praćenjem rizika IKT trećih strana uspostavlja se obveza financijskih subjekata na isključivu mogućnost suradnje s trećim stranama pružateljima usluga IKT koji osiguravaju

visoku razinu kibersigurnosti. Standardizacijom ugovornih elemenata s pružateljima usluga postiže se harmonizacija u ugovaranju ključnih elemenata poslovnih odnosa unutar cijelog financijskog sektora što bi neizravno trebalo voditi ka postizanju visoke harmonizirane zaštite i digitalne operativne otpornosti u pružanju financijskih usluga, ali moguće i poteškoćama u pronalasku odgovarajućih poslovnih partnera.

Uspostavom prvog nadzornog okvira nad pružateljima ključnih usluga IKT-a, nadležna tijela trebala bi pridonijeti ujednačenoj stabilnosti i kontinuitetu u održavanju visoke razine sigurnosti i kvaliteti pružanja financijskih usluga.

Nakon provedene analize postojećih sektorskih propisa u industriji osiguranja kao i sveobuhvatnih regulatornih zahtjeva Uredbe DORA [8], zaključuje se kako bi društva za osiguranje već trebala imati usvojene strategije i postavljene okvire za upravljanje u sigurnosti u području informacijskih i komunikacijskih tehnologija. Budući da će u narednih 18 mjeseci EBA, ESMA i EIOPA u suradnji s ESB-om i ENISA-om izrađivati zajedničke nacrte relevantnih regulatornih tehničkih standarda, društva za osiguranje trebala bi u narednom vremenskom periodu usmjeriti određene resurse prema provođenju gap analize postojećih politika, pravilnika i procedura kao i pristupiti reviziji mapiranja svih elemenata sustava IKT, a osobito dokumentiranju svih suradnji s trećim stranama pružateljima usluga IKT. Nadalje, društva za osiguranje trebala bi već sad razmotriti postojeće poslovne procese praćenja rizika IKT i metodologije procjene rizika, a osobito dodijeljene odgovornosti i ovlasti relevantnog osoblja u svrhu optimizacije postojećih procesa.

U svrhu dodatne standardizacije u pružanju visoke razine digitalne operativne otpornosti i kvalitete usluga, financijski subjekti trebali bi aktivno pratiti razvoj europskih programa kibersigurnosne certifikacije.

8. POPIS LITERATURE

[1] Europska Komisija, Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L1148 (24.09.2022.)

[2] Europska Komisija, 2020/0359 (COD), Prijedlog Direktive Europskog parlamenta i vijeća o mjerama za visoku zajedničku razinu kiberisgurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148, Bruxelles, 12 prosinca 2020 dostupno na https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN (24.09.2022.)

[3] Council of the European Union, Interinstiutional File: 2020/0359 (COD): Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148, Brussels, 17 June 2022, dostupno na https://data.consilium.europa.eu/doc/document/ST-9137-2022-INIT/en/pdf (24.09.2022.)

[4] Europska komisija, COM 2018 109 final, Komunikacija komisije Europskom parlamentu, Vijeću, Europskoj središnjoj banci, Europskom gospodarskom i socijalnom odboru i odboru regija, Akcijski plan za financijske tehnologije: za konkurentniji i inovativniji europski financijski sektor, Bruxelles, 08.03.2018. dostupno na https://eurlex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73 01aa75ed71a1.0023.02/DOC_1&format=PDF (24.09.2022.)

[5] EIOPA, ESMA, EBA, JC 2019 26, Joint Advice of the European Supervisory Authorities, To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, 20 April 2019, dostupno na https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf (24.09.2022.)

[6] Europska komisija, 2020/0266 (COD), Prijedlog Uredbe Europskog parlamenta i vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU), 24.09.2020 dostupno na https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595 (24.09.2022.)

[7] Insurance Europe, Position on the review of EU rules on the security of network and information systems (NIS2), EXCO-CS-21-049, 18 March 2021, dostupno na

https://www.insuranceeurope.eu/publications/1635/position-on-the-review-of-eu-rules-on-the-security-of-network-and-information-systems/ (24.09.2022.)

[8] European Parliament, COM2020 (0595)-C9-0304/2020-2020/0266 (COD)), Provisional agreement resulting from interinstitutional negotitations: Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 24.06.2022, dostupno na https://www.europarl.europa.eu/RegData/commissions/econ/inag/2022/07-07/ECON_AG(2022)734260_EN.pdf (24.09.2022.)

[9] Europska komisija, Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ, dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32015L2366 (24.00.2022.)

[10] Europska komisija, Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja dostupno na https://eur-lex.europa.eu/legalcontent/HR/TXT/PDF/?uri=CELEX:32009L0138&from=PL (24.09.2022)

[11] Europska komisija, Uredba (EU) br. 1094/2010 o osnivanju Europskog nadzornog tijela za osiguranje i strukovno mirovinsko osiguranje (EIOPA), dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=LEGISSUM:mi0070 (24.09.2022.)

[12] EIOPA, BoS-20/600, Smjernice o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija, dostupno na https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-gls-ict-security-and-governance-hr.pdf (24.09.2022.)

[13] Europska komisija, Direktiva 2002/21/EZ Europskog parlamenta i Vijeća od 7.ožujka 2002. o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge stavljena izvan snage 20.10.2020. godine dostupna na https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=CELEX%3A32002L0021 (24.09.2022.)

[14] Europska komisija, Direktiva (EU) 2016/97 Europskog parlamenta i Vijeća od 20. siječnja 2016. o distribuciji osiguranja, dostupno na https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=celex:32016L0097 (24.09.2022.)

[15] Službeni list Europske unije, Pročišćene verzije Ugovora o Europskoj uniji i Ugovora o funkcioniranju Europske unije, Protokoli i Prilozi Ugovoru o funkcioniranju Europske unije, Izjave priložene Završnom aktu Međuvladine konferencije na kojoj je donesen Ugovor iz Lisabona potpisan 13. prosinca 2007, dostupno na https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=celex:12016ME/TXT (24.09.2022.)

[16] Mihaljević M., Hudeček L, Časopis za kulturu hrvatskoga kljiževnog jezika, Vol.59. NO 3, 2012, dostupno na https://hrcak.srce.hr/134823 (24.09.2022.)

[17] Uredba (EU) 2019/881Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), dostupno na https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=CELEX%3A32019R0881 (24.09.2022.)

[18] EIOPA, BOS 20-002, Smjernice o izdvajanju poslova pružateljima usluga računalstva u oblaku, dostupno na https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_cor_hr.pdf (24.09.2022.)

[19] EIOPA, BOS-14-253 HR, Smjernice o sustavu upravljanja, dostupno na https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa_guidelines_on_system_of_governance_hr.pdf (24.09.2022.)

[20] Delegirana uredba Komisije (EU) 2015/35 od 10. listopada 2014. o dopuni Direktive 2009/138/EZ Europskog parlamenta i Vijeća o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II), dostupno na https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32015R0035 (24.09.2022.)

[21] Europska komisija, Uredba (EU) br. 526/2013 Europskog parlamenta i Vijeća od 21. svibnja 2013. o Agenciji Europske unije za mrežnu i informacijsku sigurnost (ENISA) i o stavljanju izvan snage Uredbe (EZ) br. 460/2004, dostupno na https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32013R0526 (24.09.2022.)

9. ŽIVOTOPIS

Tina Mazalin rođena je 1990. godine u Zagrebu. Diplomirala je 2015. godine na Pravnom fakultetu, Sveučilište u Splitu. 2017. godine završila je poslijediplomski studij iz prava informacijsko-komunikacijskih tehnologija na Pravnom fakultetu Sveučilišta u Oslu i poslijediplomski studij iz prava informacijskih tehnologija i prava intelektualnog vlasništva Pravnog fakulteta u Hannoveru. Karijeru je započela kao odvjetnička vježbenica u odvjetničkom društvu Vukmir i suradnici i u odvjetničkom uredu Tanje Petković Gregurek. Od 2018. godine do 2022. godine radila je u Croatia osiguranju d.d. na poslovima zaštite podataka i kao službenik za zaštitu podataka. Trenutno je zaposlena kao službenik za zaštitu podataka i usklađenost u Telemach Hrvatska d.o.o.

10. BIOGRAPHY

Tina Mazalin was born in 1990 in Zagreb. She graduated in 2015 from the Faculty of Law, of the University of Split. In 2017 she completed a postgraduate study in Information and Communication Technology Law at the Faculty of Law of the University of Oslo and a postgraduate study in Information Technology Law and Intellectual Property Law at the Faculty of Law of the Leibniz University Hannover. She started her career as a trainee lawyer at Vukmir and Associates and Tanja Petković Gregurek law firm. From 2018 to 2022 she has been employed at Croatia osiguranje d.d. as a Data Protection Officer. At a present time she works as a Data Protection and Compliance Officer at Telemach Croatia Ltd.