Model upravljanja informacijskom sigurnošću u usklađivanju s europskom pravnom regulativom zaštite podataka

Parlov, Natalija

SVEUČILIŠTE U ZADRU
i
LIBERTAS MEĐUNARODNO SVEUČILIŠTE

ZAJEDNIČKI POSLIJEDIPLOMSKI SVEUČILIŠNI STUDIJ
MEĐUNARODNI ODNOSI

Natalija Parlov

MODEL UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U USKLAĐIVANJU S EUROPSKOM PRAVNOM REGULATIVOM ZAŠTITE PODATAKA

Doktorski rad

Zadar; Zagreb, 2021.

SVEUČILIŠTE U ZADRU

i

LIBERTAS MEĐUNARODNO SVEUČILIŠTE

ZAJEDNIČKI POSLIJEDIPLOMSKI SVEUČILIŠNI STUDIJ
MEĐUNARODNI ODNOSI

Natalija Parlov

MODEL UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U USKLAĐIVANJU S EUROPSKOM PRAVNOM REGULATIVOM ZAŠTITE PODATAKA

Doktorski rad

Mentor

izv. prof. dr. sc. Robert Kopal

Zadar; Zagreb, 2021.

SVEUČILIŠTE U ZADRU

TEMELJNA DOKUMENTACIJSKA KARTICA

I. Autor i studij

Ime i prezime: Natalija Parlov

Naziv studijskog programa: Zajednički poslijediplomski sveučilišni studij Međunarodni odnosi

Mentor: izv. prof. dr. sc. Robert Kopal

Datum obrane: 7. lipnja 2021.

Znanstveno područje i polje u kojem je postignut doktorat znanosti: Društvene znanosti, Interdisciplinarne društvene znanosti

II. Doktorski rad

Naslov: MODEL UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U USKLAĐIVANJU S EUROPSKOM PRAVNOM REGULATIVOM ZAŠTITE PODATAKA

UDK oznaka: 004.056.53 + 34(4-67 EU)(043.5)

Broj stranica: 242

Broj slika/grafičkih prikaza/tablica: 18 / 9 / 39

Broj bilježaka: 72

Broj korištenih bibliografskih jedinica i izvora: 151

Broj priloga: 1

Jezik rada: hrvatski

III. Stručna povjerenstva

Stručno povjerenstvo za ocjenu doktorskog rada:

1. Profesor emeritus Ivo Andrijanić, predsjednik
2. Izv.prof.dr.sc. Tihomir Katulić, član
3. Doc.dr.sc. Đuro Tunjić, član

Stručno povjerenstvo za obranu doktorskog rada:

1. Profesor emeritus Ivo Andrijanić, predsjednik
2. Izv.prof.dr.sc. Tihomir Katulić, član
3. Doc.dr.sc. Đuro Tunjić, član

UNIVERSITY OF ZADAR

BASIC DOCUMENTATION CARD

I. Author and study

Name and surname: Natalija Parlov

Name of the study programme: Joint postgraduate doctoral study International Relations

Mentor: Assoc. Prof. Robert Kopal, PhD

Date of the defence: June 7, 2021

Scientific area and field in which the PhD is obtained: social sciences, interdisciplinary social sciences

II. Doctoral dissertation

Title: INFORMATION SECURITY MANAGEMENT MODEL IN COMPLIANCE WITH EUROPEAN DATA PROTECTION RULES

UDC mark: 004.056.53 + 34(4-67 EU)(043.5)

Number of pages: 242

Number of pictures/graphical representations/tables: 18 / 9 / 39

Number of notes: 72

Number of used bibliographic units and sources: 151

Number of appendices: 1

Language of the doctoral dissertation: Croatian

III. Expert committees

Expert committee for the evaluation of the doctoral dissertation:

1. Prof. Emeritus Ivo Andrijanić, PhD, chair
2. Assoc. Prof. Tihomir Katulić, PhD, member
3. Assist. Prof. Đuro Tunjić, PhD, member

Expert committee for the defence of the doctoral dissertation:

1. Prof. Emeritus Ivo Andrijanić, PhD, chair
2. Assoc. Prof. Tihomir Katulić, PhD, member
3. Assist. Prof. Đuro Tunjić, PhD, member

Izjava o akademskoj čestitosti

Ja, **Natalija Parlov,** ovime izjavljujem da je moj **doktorski** rad pod naslovom **MODEL UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U USKLAĐIVANJU S EUROPSKOM PRAVNOM REGULATIVOM ZAŠTITE PODATAKA** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 14. lipnja 2021.

Zahvala

Veliki čovjek uvijek ostane dijete.
J. W. Goethe

Od srca hvala svim mojim mentorima i prijateljima ─
vrhunskim profesionalcima ali iznad svega velikim ljudima;
na izravnosti, podršci i vjeri u mene.

Smatram to neprocjenjivim darom
i obvezujem se činiti isto.

_____

Mojoj dječici i suprugu.
Ovo je naše zajedničko postignuće.

_____

SADRŽAJ

1. Uvod

Digitalizacija i raširenost korištenja naprednih informacijskih tehnologija na globalnoj razini doveli su do sve veće važnosti uvođenja zakona i propisa povezanih s regulacijom prikupljanja i korištenja informacija.

Europsko jedinstveno digitalno tržište (*Digital Single Market* - DSM) prvi je stup Digitalne agende za Europu (*Digital Agenda for Europe* - DAE) i jedan od deset političkih prioriteta Europske komisije te predstavlja njezinu strategiju u omogućavanju građanima i pravnim subjektima da najbolje iskoriste digitalne tehnologije. Glavna je premisa DSM-a osiguranje slobodnog kretanja osoba, usluga i kapitala u čijim *on-line* aktivnostima mogu sudjelovati pojedinci i pravni subjekti po uvjetima poštene konkurencije i visoke razine zaštite osobnih podataka, kao potrošači ili pojedinaca, neovisno o njihovoj nacionalnosti ili mjestu prebivališta.

S obzirom na nove okolnosti digitalnog doba i digitalne transformacije sve većeg broja proizvoda i usluga, strategijom se želi osigurati da europsko gospodarstvo, industrija i društvo iskoriste potencijal globalnog širenja svojih mogućnosti i ukidanja regulatornih zapreka između zemalja članica Europske unije. Tijekom 2016. i 2017. godine uspješno su ukinute naknade za *roaming*, modernizirana je zaštita podataka, ostvarena prekogranična prenosivost internetskog sadržaja te dogovor o uklanjanju prepreka e-trgovini ukidanjem neopravdanog geografskog blokiranja.[1] Trenutna procjena doprinosa funkcionalnog digitalnog tržišta gospodarstvu Europske unije iznosi i do 415 milijardi eura godišnje, a do 2025. godine digitalizacija proizvodnje mogla bi donijeti 1,25 bilijuna eura, čime bi Europska unija zauzela vodeće mjesto u području svjetskih digitalnih postignuća.

Strategija DSM-a počiva na trima temeljima: pristupu, okolini te gospodarstvu i društvu, odnosno na boljem pristupu potrošačima i pravnim subjektima prema digitalnim proizvodima i uslugama na području cijele Europe, na omogućavanju jednakih uvjeta u svrhu nesmetanog

[1] Europsko vijeće, Vijeće Europske unije, *Jedinstveno digitalno tržište za Europu*. Dostupno na https://www.consilium.europa.eu/hr/policies/digital-single-market/, pristupljeno 26.1.2020. godine.

napretka digitalnih mreža i inovativnih usluga te na maksimiziranju potencijala rasta cjelokupne digitalne ekonomije.

U plasmanu svojih proizvoda i usluga, obveza je svih pravnih subjekata, kao dionika na DSM-u, i usklađenost sa svim zakonskim propisima te osiguravanje propisanih prava potrošačima, odnosno ispitanicima. Osim što može imati pravne posljedice, neusklađenost organizacija s regulativom može otežati ili posve onemogućiti daljnji izvoz ne samo na europsko jedinstveno digitalno tržište, već i na cjelokupno europsko tržište, ovisno o vrsti plasmana.

U proteklih četvrt stoljeća EU je nizom direktiva i uredbi uredila zakonski okvir zaštite osobnih podataka koji je podignut na još višu razinu, što je osobito važno i za zajedničko digitalno tržište.

Prema Dragičeviću (2015:103) „međunarodno priznanje prava na privatnost uslijedilo je u okviru Ujedinjenih naroda izglasavanjem *Opće deklaracije o ljudskim pravima*[2] 1948. godine koja propisuje da nitko ne smije biti izvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili prepisku, kao niti napadima na njegovu čast i ugled, te da svatko ima pravno na zaštitu zakona protiv ovakvog miješanja i napada.“ Lisabonski ugovor[3] i Povelja Europske unije o temeljnim pravima[4] europski su propisi koji osiguravaju najviši ustavnopravni okvir prava na zaštitu osobnih podataka, dok Konvencija Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka iz 1981. godine svjedoči o nakani europskih država da urede to područje.

U praktičnom smislu, pravni okvir zaštite osobnih podataka kao minimalni standard na području europskog tržišta daje Opća uredba o zaštiti podataka (EU) 2016/679, punog naziva Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. godine o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o

[2] UN (1948). *Opća deklaracija o ljudskim pravima*. Dostupno na: http://www.mvep.hr/custompages/static/hrv/files/081210_deklaracija_ljudska_prava.pdf, pristupljeno 11.11.2020.

[3] Europski parlament (2020). *Ugovor iz Lisabona*. Informativni članci o Europskoj uniji. Dostupno na: https://www.europarl.europa.eu/factsheets/hr/sheet/5/ugovor-iz-lisabona, pristupljeno 11.11.2020.

[4] Europska unija (2016). *Povelja Europske unije o temeljnim pravima* (2016/C 202/02). Službeni list Europske unije. Br. 202:389-405. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:12016P/TXT&from=RO, pristupljeno 12.11.2020.

stavljanju izvan snage Direktive 95/46/EZ (u daljnjem tekstu Opća uredba o zaštiti podataka ili Uredba), s pripadajućim direktivama – Policijskom direktivom, punog naziva Direktiva (EU) 2016/680 o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka i Direktivom (EU) 2016/681 o upotrebi podataka u zračnom prometu u svrhu otkrivanja terorizma i teških kaznenih djela.

Uredba je u cijelosti obvezujuća i izravno se primjenjuje u svim državama članica EU-a te je u njoj, uz ostalo, propisano i što su sve države članice bile dužne urediti u svrhu njene provedbe. Članice su pritom bile dužne osigurati zakonodavni okvir odnosno provedbene zakone. U Hrvatskoj je nacionalni provedbeni zakon odnosno Zakon o provedbi Opće uredbe o zaštiti podataka[5] (NN 42/18) (u daljnjem tekstu NPZ), koji u svojim odredbama propisuje i ona pitanja koja nisu regulirana samom Uredbom.

„Zakonom o provedbi Opće uredbe o zaštiti podataka se uređuju pojedina pitanja vezana za primjenu Opće uredbe o zaštiti podataka, a posebno: nadzorno tijelo, akreditacijsko tijelo, obrada osobnih podatka u posebnim slučajevima: privole djeteta u odnosu na usluge informacijskog društva, obrade genetskih podataka, obrada biometrijskih podataka, obrada osobnih podatka putem video nadzora kao i obrada osobnih podataka u statističke svrhe, postupci koje primjenjuje nadzorno tijelo tijekom nadzora i pravni lijekovi protiv odluka nadzornog tijela, izricanje upravnih novčanih kazni, prekršajne odredbe i upravne novčane kazne za povredu odredbi Zakona. Odredbom članka 4. Zakona, kao nadzorno tijelo u smislu odredbe iz članka 51. Opće uredbe o zaštiti podatka, određuje se Agencija za zaštitu osobnih podataka (AZOP) koja je neovisno državno tijelo, samostalno i neovisno u svojem radu.“[6]

U svrhu ujednačenja dotad decentraliziranih pravila zaštite osobnih podataka u nacionalnim zakonodavnim okvirima država članica EU, Uredbom je izričito propisano i njihovo ekstrateritorijalno područje primjene, osobito važno za *online* poslovanje i obradu osobnih

[5] Republika Hrvatska, *Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18)*, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html, pristupljeno 11.8.2020.
[6] Europska komisija (2018). Republika Hrvatska, Ministarstvo Uprave: *Pismo povjerenici Europske komisije s informacijama o stupanju na snagu nacionalnog provedbenog zakona.* Dostupno na: https://ec.europa.eu/info/sites/info/files/hr_notification_art_51.4_84.2_85.3_88.3_90.2_publish_0.pdf, pristupljeno 11.8.2020.

podataka građana EU-a (Gumzej, 2017). Prema Dragičeviću (2019:17) „Opća uredba o zaštiti podataka utvrđuje tehnološki neutralna pravila u pogledu obrade osobnih podataka pojedinca i njihova slobodna protoka. Novim pravilima nastoji se u što većoj mjeri ujednačiti europski domaći okvir zaštite osobnih podataka i što više ujednačenu te provedivu zaštitu prava potrošača u EU-u, čiji su podatci predmet tih obrada. Bitan povod za donošenje Uredbe predstavlja i potreba što učinkovitije prilagodbe europskog pravnog okvira zaštite osobnih podataka izazovima novijih tehnologija i uvjetima digitalne ekonomije koje obilježavaju sve opsežniji i kompleksniji postupci obrade podataka pojedinaca, pogotovo u umreženom globaliziranom okruženju."

Ključne odredbe Uredbe uključuju jača prava za pojedince, osobito u o*nline* okruženju, obvezu da se osiguravanje privatnosti podataka uzme u obzir pri razvoju novih tehnologija (zaštita podataka na principima predefinirane i integrirane privatnosti – *privacy by default* i *privacy by design*) te povećane ovlasti nadzornih tijela i proširenu primjenu Uredbe na sve organizacije kojima je poslovanje usmjereno na potrošače iz Europske unije. Prema Ziegler et al (2019) i Uredbi, organizacije ispitanicima moraju osigurati sva propisana prava, a koja uključuju: pravo na informiranje, pristup podatcima, ispravak podataka, njihovo brisanje, ograničenje obrade, prenosivost, povlačenje privole, prigovor i pravo na prigovor pri automatskom pojedinačnom donošenju odluka te organizacije moraju osigurati i dokazati postojanje procesa u ispunjavanju zahtjeva koje ova regulativa propisuje. Unatoč zakonskom propisu, na tržištu postoji veliki problem s pravilnim usklađivanjem organizacija i osiguravanja prava ispitanicima uslijed otežanog razumijevanja odredbi Uredbe kod velikog broja subjekata te nepostojanja unificiranog modela primjene usklađivanja. Calder i Watkins (2008) istaknuli su da zaštita podataka u kontekstu privatnosti i dostupnih tehnologija zahtijevaju složen i interdisciplinarni pristup okviru informacijske sigurnosti s obzirom na usklađenost s regulativom širom svijeta.

Prema Aksentijeviću (2014:88) „ISO/IEC 27001 je standard koji se bavi sustavom upravljanja informacijskom sigurnošću, a namijenjen je za korištenje zajedno s ISO/IEC 27002, što je praktični kodeks koji definira ciljeve sigurnosnih kontrola i preporuča određeni praktični raspon istih. On pruža praktičan model za uspostavljanje, primjenu, korištenje, praćenje, održavanje i konstantno poboljšavanje sustava za upravljanje informacijskom sigurnošću, pri čemu su dizajn i primjena pod utjecajem ciljeva poduzeća ili organizacije, procesa koji se odvijaju, te veličine i strukture same organizacije".

Standard ISO/IEC 27001 u velikom broju država podrazumijeva i postizanje određenog stupnja usklađenosti s pravnim okvirima informacijske sigurnosti. Tako primjerice Ured vijeća za nacionalnu sigurnost RH[7] organizacije koje su certificirane tim standardom spominje u kontekstu usklađenosti i s „hrvatskim propisima informacijske sigurnosti koji vrijede isključivo za neklasificirane podatke (NN 46/08, Uredba o mjerama informacijske sigurnosti, članak 8.); za zaštitu klasificiranih podataka razine ograničeno primjenjuju se, uz spomenutu normu ISO 27001 dodatno i druge mjere, a uspješna provedba norme kao što je ISO 27001, može olakšati provedbu propisanih mjera i standarda informacijske sigurnosti jer su neki sigurnosni zahtjevi slični te sama realizacija može biti lakše usklađena.“ Istovremeno, Federalni ured za informacijsku sigurnost Republike Njemačke[8] na temelju ovog standarda je omogućio organizacijama za usklađivanje s njemačkim propisima informacijske sigurnosti (IT Grundschutz). Europska je komisija ISO standarde vezane uz informacijsku sigurnost i privatnost počela sve češće preporučivati u smjernicama za postupanje s osobnim podatcima u IKT sektoru. Interdisciplinarnim pristupom funkcionalnog povezivanja zahtjeva propisanih Uredbom i nacionalnim provedbenim zakonom te procesnog okvira u aspektima organizacijskih i tehničkih mjera, zadanim kontrolama standarda ISO/IEC 27001, njegove ekstenzije ISO/IEC 27701 te konvergencijom s ISO/IEC 27002 i taksonomijom ISO/IEC 29100, napravljen je model za prepoznavanje konteksta obrada osobnih podataka u menadžmentu poslovnih procesa i načinu provođenja njihovog usklađivanja s Uredbom i nacionalnim provedbenim zakonom ili revizije usklađenosti.

1.1. Pregled dosadašnjih znanstvenih spoznaja i istraživanja

Suvremeni informacijski prostor u aspektima informacijske sigurnosti prema Klaiću (2006) obilježavaju različite klasifikacijske podjele podataka na koje treba obratiti posebnu pažnju jer se radi i o intelektualnom vlasništvu u širem smislu ali i o pravu na pristup informacijama u

[7] Republika Hrvatska, Ured vijeća za nacionalnu sigurnost (2020). *Informacijska sigurnost – NSA*, Dostupno na: https://www.uvns.hr/hr/ako-je-informacijski-sustav-uskladjen-s-hrn-iso-iec-27001-27002-je-li-uskladjen-i-s-hrvatskim-propisima-informacijske-sigurnosti-o-informacijskim-sustavima, pristupljeno 29.9.2020.
[8] Republika Njemačka, Federalni ured za informacijsku sigurnost. *IT Grundschutz*. Dostupno na: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html, pristupljeno 17.01.2021.

kontekstu elektroničke državne uprave. Lundgren i Möller (2019) ustanovili su da je definicija sigurnih podataka prema CIA pristupu ona koja podrazumijeva da je neka informacija sigurna samo ako svi dijelovi sustava u kojima se ona nalazi zadržavaju svojstva povjerljivosti, cjelovitosti i dostupnosti. Time se i pojam informacijske sigurnosti unutar organizacije odnosi na sigurnost protoka svih informacija, od informacijskog sustava, pa sve do fizičke sigurnosti dokumenata i usmenog prijenosa povjerljivih informacija. Istraživanje provedeno tijekom 2018. godine u Republici Hrvatskoj, ukazalo je na nedovoljnu informiranost malih i srednjih poduzeća o obvezi i etapama provedbe implementacije odredbi Uredbe u poslovanje, kao i nepoznavanje roka prilagodbe, kaznenih odredbi i nadležnosti institucija (Nikolić et. al, 2018).

Usklađivanje organizacije prije svega, ovisi o točnoj identifikaciji prikupljanja, obrade i arhiviranja podataka unutar sustava, o osiguravanju dostatne razine informacijske sigurnosti te legitimnosti svrhe obrade osobnih podataka. Prema Kopalu (2008) svaka organizacija, adekvatnim politikama, procedurama i drugim mehanizmima, mora uvesti tri temeljna koncepta informacijske sigurnosti: povjerljivost, integritet i dostupnost. Sustav informacijske sigurnosti mora se postaviti na način koji osigurava da samo ovlašteni korisnici mogu pregledavati i mijenjati informacije te da su informacije dostupne ovlaštenim korisnicima kad ih oni zatraže (Kim i Solomon, 2016). Uredba također predstavlja i prekretnicu u dosadašnjem korištenju naprednih marketinških metoda u prikupljanju podataka te njihovom segmentiranju i profiliranju. Prema Parlov et al (2016), značajnije se osobine bihevioralnog marketinga odnose na prilagodljivost, korisničku kontrolu, smanjenje troškova te interaktivnost. Digitalne marketinške strategije podrazumijevaju izbor odgovarajućeg sredstva digitalnog marketinga preko nekog od digitalnih kanala (Chaffey i Smith, 2008) što jasno pokazuje da se digitalni marketing oslanja na tehnologiju interneta i jedinstvene karakteristike koje donosi digitalno okruženje te na ključnu karakteristiku – mogućnost interakcije s profiliranim i identificiranim kupcem. McMillan (2002) napominje da interaktivnost utječe na stav prema pojedinoj internetskoj stranici, relevantnost teme na samoj stranici, povratak na tu stranicu, pozivanje drugih osoba na nju te kupnju s te internetske stranice. Interaktivnost značajno utječe na uspješnost e-Commercea u smislu boljeg procesuiranja informacija o samoj ponudi te bržeg donošenje odluka o samom proizvodu (Sicilia et al, 2005).

Uredba uvodi i regulaciju zaštite osobnih podataka pri aktivnostima profiliranja, a prema Rustici (2018) je u planiranju procesa koji uključuju prikupljanje i obradu podataka najvažnije

prepoznati trenutak u kojem ta obrada prelazi u profiliranje koje potom uvjetuje i obavješćivanja ispitanika te nužnost dobivanja privole samog ispitanika, obvezu izvođenja DPIA[9] analize odnosno procjene utjecaja na zaštitu podataka, mogućnost da povlačenjem privole ispitanika aktivnosti direktnog digitalnog marketinga bezuvjetno prestanu te kada i pod kojim uvjetima se podaci dijele trećim stranama. Prema Bratraneku i Kopalu (2008) anonimizirani ili pseudonimizirani podatci o pojedincima sami po sebi ne nose nikakvo značenje, niti otkrivaju osobne podatke, ali dovedeni u jednoznačnu vezu sa stvarnom fizičkom osobom predstavljaju osobni podatak koji kao takav potpada pod odredbe važeće zakonske regulative.

Razumijevanje pravnih aspekata, informacijske sigurnosti i identifikacije marketinških metoda koje uključuju osobne podatke ili moguću identifikaciju pojedinca kombinacijom različitih prikupljenih podataka, čine velik izazov organizacijama u usklađivanju. Istraživanje na području Republike Hrvatske vezano uz korištenje digitalnog i direktnog marketinga te Uredbu (Parlov et al, 2018) jasno je pokazalo da organizacije dosada nisu bile osjetljive na prikupljanje, obradu i arhiviranje osobnih podataka odnosno obrađivani osobni podaci nisu bili tretirani na način da je njihova potreba za zaštitom predstavljala značajan faktor spram koristi od njihove uporabne vrijednosti i da početak primjene Uredbe može izazvati susprezanja u često korištenim marketinškim modalitetima pri planiranju plasmana, kao i da organizacije nisu pripremljene na zahtjeve za zaštitu podataka te nisu svjesne prava koja njihovi korisnici imaju. Prema Rodrigues et al (2016), iznesen je prijedlog četiriju mogućih opcija za usklađivanje organizacija s Uredbom: (1) poticanje i potpora režima certifikacije vezane uz Uredbu; (2) akreditacija od strane certifikacijskih tijela; (3) certifikacija od strane nacionalnih nadzornih tijela te (4) kombinacija svih triju.

Usklađivanje organizacija s Uredbom korištenjem metodologije ISO/IEC 27001 sustava upravljanja informacijskom sigurnosti i njegovom ekstenzijom ISO/IEC 27701 sustava upravljanja informacijama o privatnosti, predstavlja značajan korak u olakšavanju usklađivanja organizacija s ovom pravnom regulativom.

[9] Procjena utjecaja na privatnost (*Data Protection Impact Assessment DPIA)* – analiza koja je uvjet za bilo koju vrstu obrade osobnih podataka koja bi mogla rezultirati velikim rizikom za prava i slobode pojedinaca.

1.2. Cilj i hipoteze istraživanja

Opća uredba o zaštiti podataka kao opći normativni tekst ne nudi procesno primjenjiv način za usklađivanje poslovnih procesa organizacija sa svojim zahtjevima. Kao model primjene za usklađivanje poslovnih procesa s Uredbom i nacionalnim provedbenim zakonom moguće je koristiti kombinaciju izdvojenih međunarodnih ISO standarda vezanih uz informacijsku sigurnost, privatnost i tehnike auditiranja. Glavni su ciljevi disertacije utvrditi utječe li izostanak modela primjene na proces implementacije usklađenosti s Uredbom i u kojoj bi mjeri korištenje bazne metodologije ISO/IEC 27001 standarda u formiranju modela primjene facilitiralo usklađivanje poslovnih procesa organizacija s Uredbom te izraditi model za prepoznavanje konteksta obrada osobnih podataka u menadžmentu poslovnih procesa i načinu provođenja njihovog usklađivanja s Uredbom ili revizije usklađenosti.

U skladu s navedenim ciljevima postavljaju se sljedeće hipoteze:

H1 Izostanak procesno primjenjivog modela usklađivanja organizacija s Uredbom povezan je s njihovim otežanim usklađivanjem ili potpunim izostankom usklađivanja

H2 Korištenje ISO/IEC 27001 pri ispunjavanju propisanih zahtjeva za zaštitom osobnih podataka olakšava usklađivanje organizacija s Uredbom

H3 Veličina tvrtke (broj zaposlenih) i kompleksnost obrade osobnih podataka povezani su s načinom usklađivanja organizacija s Uredbom

1.3. Plan i metodologija istraživanja

Kako bi se ispunili ciljevi doktorske disertacije kabinetskim se metodama istraživanja sekundarnih izvora (dostupne stručne i znanstvene literature te javno dostupnih podataka, kao i postojećih pravilnika, uredbi i standarda) ustanovilo postojeće stanje u implementaciji usklađenosti s Uredbom na subjektima u Republici Hrvatskoj, analizirala metodologija ISO standarda, te upotreba ISO/IEC 27001 standarda kao modela primjene za usklađivanje procesa s Uredbom u organizacijama. Pritom je korištena deskriptivna metoda, te metode analize, sinteze i dedukcije.

Teorijska poglavlja disertacije temelje se na sekundarnim izvorima kao što su: knjige, znanstveni i stručni članci, zbornici znanstvenih i stručnih konferencija, znanstveni magistarski radovi i doktorske disertacije, javno dostupni podatci, studije slučaja, pravilnici, zakoni i standardi kao i priručnici i dokumentacija za njihovu primjenu, te internetski izvori. Obveze po zaštiti podataka i pravima ispitanika, propisane u člancima Uredbe, dobile su propisni način primjene u ispunjenju zahtjeva putem interpretacije i kombinacije zahtjeva iz izdvojenih ISO i ISO/IEC standarda te *vice versa*.

Provedeno je primarno istraživanje na uzorku organizacija u Hrvatskoj pri čemu su korištene metode anketnog istraživanja (ankete) i matematičko-statističke metode.

Istraživačka poglavlja disertacije temelje se na provođenju internetske ankete kojom se utvrdio stupanj implementacije usklađenosti s Uredbom, kao i ostale varijable povezane s njime, te postojanje različitih ISO standarda, između ostaloga i ISO/IEC 27001 u organizacijama. U anketiranju je korišten strukturirani kvantitativni upitnik koji je prethodno testiran kroz intervjue odnosno razgovore s predstavnicima pojedinih organizacija.

Pitanja u anketnom upitniku podijeljena su u sljedeće skupine:

- Opći podatci o organizaciji (veličina, regija)
- Vrste osobnih podataka koje organizacija prikuplja, obrađuje i arhivira te rok čuvanja podataka

- Metode digitalnog i klasičnog marketinga koje organizacija koristi u prikupljanju i daljnjem korištenju podataka
- Načini zaštite informacijskog sustava unutar organizacije
- Trenutna razina implementacije usklađenosti s Uredbom
- Razumijevanje članaka Uredbe
- Način i brzina uvođenja usklađenosti s Uredbom
- Korištenje usluga vanjskih suradnika/konzultanata
- Postojanje ISO standarda u organizaciji
- Percepcija ISO standarda, osobito ISO/IEC 27001 standarda kao modela primjene usklađenosti s Uredbom
- Poslovanje sa zemljama EU-a.

Anketa je provedena putem interneta, pozivanjem relevantnih ispitanika u organizacijama za koje postoje kontakt podatci te putem objava na medijskim kanalima, a dio ispitanika prikupljen je postavljanjem poziva na mrežnim stranicama i društvenim mrežama. Relevantni ispitanici klasificirani su kao odgovorne osobe u organizacijama ili osobe unutar organizacija zadužene za usklađivanje s europskom pravnom regulativom. Također je korištena metoda snježne grude (*snowball*) koja podrazumijeva da ispitanici proslijede poziv na istraživanje ostalim potencijalnim ispitanicima. Ovako definiran uzorak je prigodni uzorak, no kako je i sama populacija, odnosno mogući bazen (*pool*) ispitanika relativno ograničen, način uzorkovanja predstavlja valjani način prikupljanja podataka. Očekivani uzorak iznosio je 100 ispitanika, što je dostatno reprezentativan dio ispitivane populacije.

Podatci dobiveni anketnim istraživanjem analizirani su različitim statističkim kvantitativnim postupcima. U analizi kvantitativnih podataka najprije su izračunati osnovni deskriptivni pokazatelji (postotci odgovora, mjere centralne tendencije, mjere raspršenja, normalnost distribucije). Nadalje su, sukladno parametrima dobivenim deskriptivnom analizom, podatci analizirani različitim statističkim parametrijskim i neparametrijskim metodama. Konkretno, analizom smjera, veličine i značajnosti povezanosti između dobivenih podataka (korelacija) te regresijskim modeliranjem analizirano je postojanje i priroda povezanosti između pojedinih varijabli. Također, u svrhu testiranja statističke značajnosti razlika između rezultata različitih

podskupina ispitanika korišteni su parametrijski (t-test, analiza varijance) i neparametrijski (Hi-kvadrat) testovi. Razina statističke značajnosti određena je na manje od 5 % ($p < 0,05$), što je standardna granična vrijednost u istraživanjima ovoga tipa.

Istraživanje je provedeno putem internetskog upitnika, a u pratećem dopisu/tekstu poziva na sudjelovanje u istraživanju pojašnjeni su cilj i svrha istraživanja. Posebno je naglašena anonimnost sudjelovanja i korištenje prikupljenih podataka isključivo u znanstvene svrhe. Uz navedeno, pojedina su pitanja dodatno pojašnjena u samom upitniku kako bi se osiguralo razumijevanje i sagledavanje istraživačkih pitanja, a time i dobivanje što potpunijeg i preciznijeg odgovora.

Uz navedeni anketni upitnik, provedeni su i dubinski intervjui s ekspertima iz privatnih organizacija koje nude konzultantske usluge u primjeni i implementaciji usklađenosti s Uredbom. Kao vodič za dubinske intervjue korišten je polustrukturirani upitnik čije teme su obuhvatile:

- razinu poznavanja zaštite informacijskih sustava
- razinu razumijevanja vrste i načina prikupljanja i obrade osobnih podataka marketinškim metodama
- percepciju stanja u implementaciji usklađenosti s Uredbom u hrvatskim organizacijama
- probleme i zapreke na koje se nailazi u hrvatskim organizacijama prilikom implementacije usklađenosti s Uredbom
- razinu razumijevanja Uredbe u hrvatskim organizacijama
- potrebe za modelom primjene u implementaciji usklađenosti s Uredbom, te potencijal ISO/IEC 27001 kao modela primjene.

Analiza dubinskih intervjua provedena je kvalitativnom metodom i služi kao dopuna i pojašnjenje podataka i analiza dobivenih iz primarnih i sekundarnih izvora.

U disertaciji je iznesen i opći okvir za uspostavljanje i implementaciju usklađenosti organizacija s Uredbom putem modela primjene temeljenog na ISO/IEC 27001 standardu međunarodnih

sustava upravljanja informacijskom sigurnosti te na njegovoj ekstenziji ISO/IEC 27701 sustava upravljanja informacijama o privatnosti.

1.4. Znanstveni doprinos

Teorijski doprinos

Europsko je jedinstveno digitalno tržište, zahvaljujući e-trgovini i e-upravi, jedan od najvažnijih pokretača europskog gospodarstva. Zbog značajnih promjena uvjetovanih novim načinom pružanja usluga ili plasmana proizvoda uslijed digitalne transformacije poslovanja donesen je regulatorni okvir koji ne ovisi o državnim granicama i usmjeren je ka zaštiti privatnosti te informacijskoj i kibernetičkoj sigurnosti. Opća uredba o zaštiti podataka (Uredba, GDPR) u svakom nacionalnom pravnom sustavu zemlje članice EU primjenjuje se neposredno.

Sekundarna istraživanja bila su usmjerena na aspekte multifacetne prirode digitalne transformacije i njenog potencijala u različitim industrijama te orijentiranosti EU ka standardizaciji i normizaciji korištenjem ISO metodologije. Prikupljeni su podaci o DESI indeksu gospodarske i društvene digitalizacije u EU i RH, glavnim aspektima strategije EU i potencijalu europskog jedinstvenog digitalnog tržišta te su identificirani preferirani ISO standardi vezani uz informacijsku sigurnost, privatnost i provođenje revizije.

Primarno istraživanje bilo je usmjereno na (1) identifikaciju ključnih parametara utjecaja na razinu razumijevanja zahtjeva propisanih Uredbom, (2) parametara vezanih uz razinu težine usklađivanja poslovnih procesa sa zahtjevima Uredbe u odnosu na korištenje metodologije ISO standarda i (3) orijentiranosti izvozu na EU tržište.

Prikupljeni su podaci hrvatskih organizacija o karakteristikama obrada osobnih podataka u menadžmentu poslovnih procesa i njihove zaštite u digitalnom okruženju; trenutnoj razini, načinima i faktorima koji utječu na težinu usklađivanja njihovih poslovnih procesa s Uredbom te postotak izvoza na europsko tržište u odnosu na ukupni tržišni plasman poduzeća.

Priznatim znanstvenim metodama ustanovljena je međupovezanost između (1) razumijevanja zahtjeva propisanih Općom uredbom o zaštiti podataka (Uredba EU 2016/679) i (2) nedostatka smjernica za usklađivanje poslovnih procesa s Uredbom te je ustanovljena i orijentiranost plasmanu na europsko tržište.

U teorijskom smislu znanstveni doprinos ogleda se u iznalaženju jedinstvenog sveobuhvatnog unificiranog modela za prepoznavanje konteksta obrada osobnih podataka u menadžmentu poslovnih procesa i načina provođenja usklađivanja organizacijskih i tehničkih mjera s Uredbom i hrvatskim nacionalnim provedbenim zakonom ili revizije usklađenosti.

Navedeni model do sada ne postoji ni u teorijskom ni u aplikativnom smislu, a primjenjiv je u provedbi usklađivanja poslovnih procesa s Uredbom i nacionalnim provedbenim zakonom u aspektima zahtjeva vezanih uz organizacijske i tehničke mjere te provedbi revizije usklađenosti, što čini i njegov aplikativni doprinos.

Aplikativni doprinos

Sukladno integriranim rezultatima provedenih istraživanja napravljen je primjenjiv opći okvir za strukturirano uspostavljanje, usklađivanje i provođenje revizije usklađenosti organizacijskih i tehničkih mjera s Uredbom i nacionalnim provedbenim zakonom.

Uredba sadrži skup zahtjeva bez jasnih uputa i smjernica kako ih ostvariti. Model se temelji na metodologiji kompilacije i deduktivne logike u kombiniranju izabranih ISO i ISO/IEC standarda i zahtjeva predmetnih zakona te predstavlja integrirani sustav jasnih smjernica, kontrola i načina evaluacije razine usklađenosti organizacijskih i tehničkih mjera u menadžmentu poslovnih procesa.

U modelu je uspostavljen funkcijski odnos između zahtjeva propisanih Uredbom i nacionalnim provedbenim zakonom, kontrola i zahtjeva propisanih međunarodnim standardima informacijske sigurnosti i privatnosti ISO/IEC 27001 i ISO/IEC 27701, kodeksa postupanja s kontrolama informacijske sigurnosti ISO/IEC 27002, taksonomije okvira za uspostavljanje

zaštite privatnosti propisanog standardom ISO 29100 te tehnika auditiranja propisanih međunarodnim standardom ISO 19011.

Korištenje modela organizacijama omogućava olakšano razumijevanje i usklađivanje poslovnih procesa sa zahtjevima propisanim Uredbom i nacionalnim provedbenim zakonom te otklanja potencijalnu prepreku u plasmanu proizvoda i usluga na europsko tržište omogućujući olakšano dokazivanje usklađenosti s ovom regulativom putem dokumentirane informacije.

1.5. Struktura disertacije

Ova disertacija sastoji se od sedam (7) cjelina odnosno poglavlja te popisa literature i izvora podataka, sažetka na hrvatskom i engleskom jeziku, popisa grafikona, slika i tablica, priloga te životopisa na njezinu kraju.

U prvom poglavlju, *Uvodu*, predstavljen je strateški kontekst disertacije koji uključuje pregled dosadašnjih znanstvenih spoznaja i istraživanja po predmetnoj tematici, cilj i hipoteze istraživanja, plan i metodologija istraživanja te znanstveni doprinos i struktura same disertacije.

U drugom se poglavlju pod nazivom *Teorijski aspekti digitalne ekonomije i zaštita osobnih podataka*, teorijski obrađuju i analiziraju pojmovi digitalne ekonomije i potencijala digitalne transformacije u različitim industrijama, DESI Indeksa gospodarske i društvene digitalizacije, Digitalne Agende za Europu (DAE) te europskog Jedinstvenog digitalnog tržišta. Analizirani su podaci dobiveni sekundarnim istraživanjima u aspektima DESI indeksa gospodarske i društvene digitalizacije u EU i RH, glavnih aspekata Strategije EU 2020 i potencijala europskog jedinstvenog digitalnog tržišta te je iznesen i pregled hrvatskih pokazatelja u odnosu na ostale zemlje EU-a.

Treće poglavlje pod nazivom *ISO standardi* sadrži kratak povijesni pregled i djelokrug Međunarodne organizacije za standardizaciju kao krovnog tijela za donošenje standarda te su analizirani podaci dobiveni sekundarnim istraživanjima s obzirom na Strategiju ISO-a,

raširenost najzastupljenijih certifikacija sustava upravljanja i njihovu distribuciju prema vrsti certifikata, zemlji i industriji s posebnim fokusom na certifikaciju standarda ISO/IEC 27001 u svijetu i Hrvatskoj. Analizirane su europske smjernice o standardizaciji i normizaciji te su izdvojeni preferirani ISO standardi vezani uz informacijsku sigurnost i privatnost te provođenje revizije na kojima počiva strategija izrade samog modela.

Četvrto poglavlje, *Model procjene sustava upravljanja informacijskom sigurnošću i privatnošću u analizi stanja i reviziji usklađenosti organizacijskih i tehničkih mjera postojećeg sustava s ISO/IEC 27001 i ISO/IEC 27701 i/ili Općom uredbom o zaštiti podataka*, sadrži cjelokupni opis strukture i metodologije predloženog NPISPMSA modela integriranog sustava pet ISO/IEC standarda za provedbu analize stanja i revizije usklađenosti organizacijskih i tehničkih mjera u menadžmentu poslovnih procesa. Analizirani su taksonomija i strukture standarda te je definiran analitički proces s klasifikacijama razina usklađenosti i evidentirana potrebna ekspertna znanja za provođenje postupka analize ili revizije. Iznesene su mogućnosti certifikacije cjelokupnog sustava pri implementaciji sustava upravljanja informacijskom sigurnošću i privatnošću putem tog modela. Poglavlje sadrži i verifikaciju modela s detaljnim opisima uvjeta testiranja i rezultatima vrednovanja koji potvrđuju da je primjenom predložene metode ostvaren aplikativni doprinos.

Peto poglavlje, *NPISPMSA model*, predstavlja aplikativni doprinos ove disertacije i sadrži cjelokupni sadržaj modela procjene sustava upravljanja informacijskom sigurnošću i privatnošću u analizi stanja i reviziji usklađenosti organizacijskih i tehničkih mjera postojećeg sustava s Uredbom i nacionalnim provedbenim zakonom ili kontrolama proširenog ISO/IEC 27001 sustava upravljanja informacijskom sigurnosti.

Šesto poglavlje pod nazivom *Prikaz i analiza rezultata istraživanja* sadrži glavno istraživačko poglavlje rada gdje su predstavljeni rezultati primarnog istraživanja odnosno definirani su metodologija i uzorak te je iznesena cjelokupna statistička analiza podataka s provjerom povezanosti zadanih varijabli te testiranjem i dokazivosti postavljenih hipoteza. Sukladno Hipotezi 1 provjeren je odnos percipirane težine usklađivanja s Općom uredbom o zaštiti podataka preko tri pokazatelja koji izravno ukazuju na potrebu za uvođenjem procesno primjenjivog modela koji bi olakšao usklađivanje organizacija s Uredbom. Hipoteza 2 vezana uz utjecaj korištenja ISO certifikata na implementaciju usklađenosti s Općom uredbom o zaštiti

podataka testirana je u dva dijela odnosno dio u kojem se provjerava utjecaj na težinu usklađivanja s Uredbom i dio u kojem je provjereno koliko posjedovanje ISO/IEC 27001 pomaže u organizaciji poslovanja. U sklopu Hipoteze 3 provjereni su odnosi varijabli veličine organizacija, broja zaposlenih, korištenja ISO sustava, korištenja usluga vanjskih konzultanata i percepcije težine usklađivanja s Općom uredbom o zaštiti podataka. Istovremeno je provjerena i povezanost kompleksnosti obrade osobnih podataka s korištenjem ISO sustava upravljanja, usluga vanjskih konzultanata kao i percepcijom težine usklađivanja s Općom uredbom o zaštiti podataka. Na kraju poglavlja predstavljeni su i rezultati analize vezani uz dodatna pitanja o poslovanju anketiranih hrvatskih poduzeća sa zemljama Europske unije.

Sedmo poglavlje, *Zaključak*, sadrži sažete rezultate disertacije te su još jednom navedeni njezin problem i predmet, ciljevi, hipoteze i primijenjene metode, kao i kratki opis predloženog verificiranog modela.

Nakon *Zaključka* slijede popisi izvora i korištene literature, sažetak i ključne riječi na hrvatskom i engleskom jeziku te popis grafikona, slika i tablica, prilog (anketni upitnik) i životopis autorice.

2. Teorijski aspekti digitalne ekonomije i zaštita osobnih podataka

2.1. Digitalna ekonomija i potencijal digitalne transformacije

I u digitalno doba, davno utemeljeni ekonomski postulati vezani uz samoregulaciju tržišta i „nevidljivu ruku“ Adama Smitha[10] te pojam učinkovitosti tržišta kojeg su Samuelson i Nordhaus (2005:5) definirali kao „ekonomsku korist koja dolazi od radnji pojedinaca koji se brinu za svoj vlastiti interes“ nisu se promijenili. Smith je pojam nevidljive ruke destilirao kroz dvije kritičke ideje: (1) dobrovoljno trgovanje na slobodnom tržištu donosi nenamjerne i raširene koristi i (2) te koristi veće su od koristi regulirane ekonomije. Elastičnost ponude i potražnje i dalje djeluje na istovjetan način; upravo zato što se psihologija čovjeka i temeljni mehanizmi njegovog odlučivanja o kupnji nisu promijenili. Promijenilo se to da su informacije o ponudi predmeta njegove želje dostupnije na način koji je brži i lakši no ikad, kao i to da je njegovo ponašanje u smislu analize potražnje pritom postalo neprocjenjiva informacija koja se konstantno ažurira i koju je moguće lako pratiti tijekom vremena te njenom agregacijom predvidjeti buduću potražnju, a samim time i kreirati buduće trendove i prilagoditi ponudu što je u marketingu neprocjenjiv doprinos.

Slijedom toga, digitalna ekonomija se prema Romanelliju (2019) ne može razmatrati u kontekstu jedinstvene definicije već kombinaciji ekonomskih aktivnosti, komercijalnih rtansakcija i komunikacije putem IKT-a, a prema Strømmen-Bakhtiar (2019:7) ona se odnosi na aktivnosti koje se temelje na „raširenoj upotrebi informacijske tehnologije (hardver, softver, aplikacije i telekomunikacije) u svim aspektima ekonomije, uključujući unutarnje poslovanje organizacija (posao, vladu i neprofitne organizacije), transakcije između organizacija i transakcije između pojedinaca, djelujući i kao potrošači i kao građani“. Aspekti digitalnog opsežno su izučavani i početkom 2000-ih te je još Petersen (2003:114) „novu ekonomiju identificirao pojmom „virtualna ekonomija“ uslijed jačanja uloge nematerijalnih resursa i ostale neopipljive imovine te nestanka klasično organiziranih poduzeća te nepostojanja fizičke nazočnosti tijekom poslovnih odnosa“. Istovremeno ekonomske mogućnosti vezane uz „sve

[10] Smith, Adam, 1723-1790. (1994). *An inquiry into the nature and causes of the wealth of nations*. New York : Modern Library

raširenije internetsko poslovanje ukazuju na sve opipljivije brisanje granica u međunarodnom poslovanju“ (Kolaković, 2006:157), a uzrokovale su i „viši stupanj internacionalizacije poduzeća, kao i povećanja broja međunarodnih aktivnosti“; koji prema Mikić et al (2016:1205) neminovno vode i ka „boljem postizanju poslovnih rezultata“.

Goldfarb i Tucker (2017) zaključili su da ekonomski efekti koje uzrokuje raširena upotreba digitalne tehnologije ne zahtijevaju novu ekonomsku teoriju iz korijena nego drugačije naglaske s obzirom na novu definiciju kapitala koju predstavlja sama informacija o mogućnosti praćenja ponašanja potrošača; Floridi (2018) je zaključio da se sama revolucija već dogodila i da je neophodno preispitati postojeće i definirati primjerene etičke norme s obzirom na novo stanje i mogućnosti. Sve to upućuje na zaključak kako je „informacija“ jedan od glavnih resursa digitalnog doba, što su prepoznali i Lazibat i Kolaković (2004:141) i utvrdili da su u „suvremenoj globalnoj ekonomiji znanje i intelektualni kapital su ključni čimbenici poslovanja dok osnovicu suvremenog razvoja, a samim time i trgovine, čini informacija kao novi nematerijalni resurs“. Istovremeno „velike kompanije poput Googlea, Applea, Amazona, Facebooka, Tencenta, Alibabe, Baidua i sličnih servisa svojim disruptivnim inovacijama diktiraju karakter suvremene ekonomije, kao i novog načina života“ (Ivanković, 2018:8), a sama digitalna se ekonomija uslijed te pojavnosti definira i ekonomijom čiji temelj su IKT tehnologijame u svojstvu sredstva komunikacije i stvaranja vrijednosti (Guerra Guerra et al., 2019).

No digitalna ekonomija u samom svom korijenu podrazumijeva i digitalnu transformaciju te prateći regulatorni okvir koji neminovno kasni za tehnološkim mogućnostima koje su u opticaju te su svakim danom sve naprednije. Tako pojam informacijske sigurnosti i zaštite podataka dobiva sve veću važnost jer nije riječ samo o „problemu“ sektora informacijsko-komunikacijskih tehnologija, već i značajnom izazovu u regulaciji zaštite osobnih podataka s obzirom na to da su upravo oni glavni pokretač i predmet interesa u mogućnostima prediktivne analitike u predviđanju trendova u ponudi i potražnji.

Značajan dio informacijske sigurnosti u digitalnoj ekonomiji u velikoj se mjeri tiče informacijsko-komunikacijskih tehnologija s obzirom na sve aspekte protoka informacija digitalnim putem koji se tiču hardverskih, mrežnih i softverskih aspekata, dok se njezin drugi dio tiče fizičkih aspekata. Awad i Fairhurst (2018) su napomenuli da je sigurnost informacija

postala presudna potreba u zaštititi aplikacija vezanih uz informacijske transakcije koja zaslužuje sinergiju informatičke i inženjerske zajednice.

Uslijed sve većeg širenja informacijskih i komunikacijskih tehnologija pojam informacijske sigurnosti obuhvaća i teme poput sigurnosti i privatnosti vezane uz pametne gradove, sigurnosti računalstva u oblaku, zdravstva, sigurnosti Interneta stvari (IoT) (King i Awad, 2016), sigurnosti Interneta vozila i nekoliko vrsta sigurnosti bežičnih senzorskih mreža (Grzenda et al, 2017). Uz to, informacijska sigurnost se proširila ne samo na aspekte vezane uz probleme tehničke sigurnosti već i na izazove organizacijske i socijalne sigurnosti (Charif i Awad, 2014).

Prema Bloombergu (2018), prva etapa u postizanju digitalne transformacije jest digitizacija koja podrazumijeva proces prijelaza iz analognog u digitalni oblik rada odnosno stvaranje digitalnih verzija stvari dostupnih u fizičkom obliku. I dok se digitizacija više odnosi na same sustave zapisivanja podataka, digitalizacija predstavlja unaprjeđenje i transformaciju poslovnih operacija i funkcija te procesa i aktivnosti kojima se utire put digitalnoj transformaciji i poslovanju u digitalnoj ekonomiji (Igrec, 2018). Iz svega navedenog razvidno je da je digitalizacija proces razmjene samih informacija između uređaja te njihovo međusobno povezivanje pomoću različitih tehnologija (Spremić, 2017).

„Digitalna transformacija podrazumijeva intenzivnu primjenu digitalne tehnologije i resursa kako bi se ti resursi pretvorili u nove prihode, poslovne modele i načine poslovanja te nastaje kada poduzeće odluči u relativno kratkom vremenskom razdoblju iz temelja mijenjati svoje poslovne procese, strategije, aktivnosti, hijerarhijsku i organizacijsku strukturu, sve kako bi se ti procesi i strategije bolje povezali i na kraju krajeva omogućili bolju konkurentsku prednost poduzeću na tržištu“ (Liu et al, 2011:7). Ona zahtijeva promjenu strategije poslovanja u skladu sa stalnim tehnološkim napretkom uslijed kojeg organizacija smanjuje svoje troškove poslovanja povećavajući profitabilnost standardizacijom i unaprjeđenjem procesa. U procesu informatizacije treba razmišljati i o troškovnom aspektu vezanom uz informacijsku sigurnost te planirati te troškove s obzirom na koristi koje ona može donijeti (Charif i Awad, 2016).

Pojam digitalne ekonomije služi predstavlja „nove modele u poslovanju uz nove aspekte u dizajnu proizvoda i usluga, kao i tržišta koja predstavljaju brzorastuće sektore ekonomije koji se temelje na digitalnim tehnologijama kao osnovnoj infrastrukturi poslovanja dok njen koncept

počiva na pet ključnih principa: (1) integraciji i istodobnoj primjeni neovisno razvijenih tehnologija i mogućnosti koje one pružaju, (2) integraciji progresivnih koncepcija poslovanja, (3) korištenju digitalnih platformi poslovanja, (4) uspješnim i „neodoljivim" digitalnim poslovnim modelima te (5) vođenju temeljenom na poduzetničkoj organizacijskoj kulturi, inovativnosti i stvaranju nove vrijednosti" (Spremić, 2017:30).

Digitalna transformacija poslovnih procesa u organizacijama istovremeno je transformirala i njihov način tržišnog nastupa s obzirom na proširene tehnološke mogućnosti, ne samo u plasmanu proizvoda i usluga digitalnim putem nego i u oblikovanju naprednih marketinških strategija koje su uključivale praćenje kupovnih navika svojih ciljnih skupina temeljenih na izuzetno kvalitetnoj, u realnom vremenu dostupnoj te cjenovno prihvatljivoj analitičkoj podlozi. Kvalitetna analitička podloga interaktivnog praćenja kupovnih navika ciljnih skupina i predviđanja buduće potražnje temelji se na deduktivnoj metodi prikupljanja i obrade podataka prikupljenih digitalnim kanalima, a završava na krajnjem ishodu koji predstavlja najveću vrijednost – osobnom podatku.

Zbog mogućnosti predviđanja potražnje, organizacije su sve više orijentirane na poslovni model koji počiva na bioničkoj transformaciji, odnosno modelu koji „odgovara na potražnju kupaca" ciljajući upravo na krajnju instancu – kupca kao jedinstvenu fizičku osobu, a ne više na klasičnom upravljanju ponudom proizvoda i usluga što odgovara konceptu bioničke transformacije. Prema Kasahari (2018) postoje tri oblika kapitala bioničke transformacije: bihevioralni, kognitivni i mrežni od kojih (1) bihevioralni kapital podrazumijeva prikupljanje, agregiranje i modeliranje podataka na način da on može dati vrijedan i provjerljiv rezultat (uvid) prikupljanjem podataka putem IoT, senzora, surfanja, korištenja mobilnih aplikacija i slično te prikazuje aktivnost ponašanja ljudi, strojeva i sustava u realnom vremenu otkrivajući kako su se ponašali u prošlosti, kako će se vjerojatno ponašati u budućnosti i kako se na to ponašanje može utjecati; (2) kognitivni kapital podrazumijeva imovinu koja dobiva na vrijednosti zahvaljujući svojoj „izračunljivosti" odnosno automatizaciji kognitivnih zadataka te predstavlja razvrstavanje informacija iz baze znanja u različite cjeline; i (3) mrežni kapital podrazumijeva informacije vezane uz načine na koje organizacije (i privatne i javne) povezuju svoje kupce, korisnike, zaposlenike i druge aktere uslijed generiranja određenih vrsta i kategorija podataka koji mogu imati veliku vrijednost po samu organizaciju i unaprjeđenje postojećih procesa ili kreiranje novih proizvoda i usluga.

Digitalna transformacija zahvatila je sve industrije i na taj način utjecala na promjene u ekonomiji i cjelokupnom društvu. Budući da se radi o sveprisutnom i progresivnom procesu, niti jedan sektor nije ostao netaknut digitalnom transformacijom, ali se razlike u brzini inkorporiranja i područjima širenja promjena među industrijama značajno razlikuju. Digitalna je transformacija proces koji počinje planiranjem uvođenja digitalnih tehnologija u poslovanje i završava njihovom potpunom integracijom. Proces uključuje sve zaposlenike i njihovu interakciju sa svim zainteresiranim stranama organizacije na području informiranja o proizvodima i uslugama, podrške u odlučivanju, procesu kupnje i povratnim informacijama o korisničkom iskustvu. Prema nekim autorima, rast tehnološkog razvoja u industriji 4.0 je eksponencijalan te je zbog toga teže predvidjeti i izazove i dobrobiti nego što je to bilo s prethodnim industrijskim revolucijama (Morrar et al, 2017). Kada se govori o poboljšanjima koje digitalna transformacija može donijeti redovito se spominju povećanje učinkovitosti, razvoj ekosustava poduzeća, povećanje agilnosti, proaktivno reagiranje na poremećaje redovitih poslovnih modela, stvaranje konkurentske prednosti, kreiranje novih tržišta, proizvoda ili usluga, upravljanje korisničkim iskustvom (Pejić Bach et al, 2017; Dhawan et al, 2018).

Da bi se mogle razumjeti razlike u utjecaju digitalne transformacije na različite proizvodne i uslužne aktivnosti, nužno je krenuti od multifacetne prirode digitalne transformacije. Prema recentnim OECD istraživanjima (Calvino et al, 2018) kod procjene i usporedbe digitalne transformacije u industrijama potrebno je u obzir uzeti tri sastavnice: (1) tehničke komponente digitalizacije kao što su investicije u IKT, kupnja IKT proizvoda i usluga, robotizaciju, zatim (2) ljudski kapital potreban za uključivanje tehnologije u proizvodnju i konačno (3) ulogu koju digitalna tehnologija ima u interakciji tvrtki s tržištem, odnosno *on-line* prodaju.

Suvremeni uvjeti poslovanja sve više su pod utjecajem povećane dinamike i kompleksnosti okruženja koji otežavaju upravljanje poslovnim procesima što povećava neizvjesnost u svakom segmentu poslovanja koja uzrokuje da se i sam menadžment sve više usmjerava na upravljanje poslovnim rizicima (Andrijanić et al, 2016), dok su u skladu s tim rast vrijednosti poduzeća i njegov opstanak na tržištu sve ugroženiji s obzirom na izloženost raznim oblicima poslovnih rizika koji su također proširenog spektra. "U međunarodnom poslovanju čitav problem dodatno potencira različitost ekonomskih i neekonomskih rizika zemlje" (Andrijanić i Pavlović, 2016:208). U svezi s tim zaključcima, ranije je uočeno (Spremić i Hlupić, 2007) i da se sama

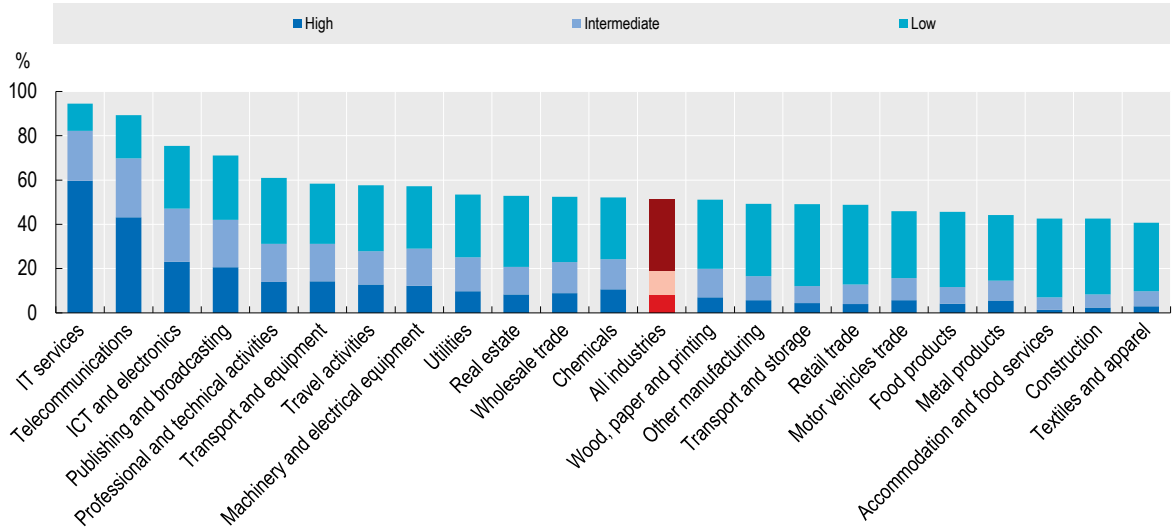
praksa upravljanja informatikom na razini menadžmenta, koju sad pak nalaže digitalna transformacija, značajno razlikuje među kompanijama i ovisi o definiranosti same uloge informatike u poslovanju odnosno dodijeljene odgovornosti za donošenje odluka vezanih uz informatiku. Ladley (2012) je pritom istaknuo i da upravljanje podatcima treba provoditi u etapama i pažljivo dizajniranom okruženju. Ne treba zanemariti niti stavku da su ljudi i procesi jednako važni za postizanje optimalne sigurnosti u modernom poduzeću, dok dobro upravljanje zahtijeva i opsežnu suradnju multidisciplinarnih timova (Vacca, 2017).

2.1.1. Industrije: prihvaćanje i posljedice digitalne transformacije

Prema analizama OECD-a temeljenim na podatcima Eurostata objavljenim u siječnju 2019. godine (Eurostat, 2019), europska poduzeća još uvijek nisu iskoristila puni potencijal digitalne transformacije. Uzimajući u obzir sve tri sastavnice, 50 % svih europskih poduzeća u privatnom sektoru (isključujući tvrtke u sektoru financija), interno ne raspolaže s dostatnim IKT kapacitetima, a samo 20 % je procijenjeno kao srednje sposobno. Kapacitiranost industrija se znatno razlikuje pa je u sektorima IT usluga i telekomunikacija 40 % do 80 % poduzeća u kategoriji srednje/umjereno razvijenih dok je u tehnološki manje razvijenim industrijama, kao što su proizvodnja tekstila i odjeće te usluge transporta i skladištenja, samo 10 % poduzeća u srednjoj kategoriji razvijenosti.

Slika 1. Poduzeća s internim IKT kapacitetima prema industrijama, zemlje EU, 2018.

% poduzeća s deset i više zaposlenih osoba u svakoj od industrija



Izvor: Eurostat, OECD (2019)

Prema referentnim vrijednostima u područjima tehničkih komponenti digitalizacije, ljudskih kapaciteta i interakcije s tržištem, vodeći su sektori IKT-a, putovanja, trgovina na veliko, dok relativno najviše zaostaju sektori građevinskih usluga, prehrambene i prerađivačke industrije. Industrije se razlikuju i prema stupnju razvijenosti sastavnica digitalizacije. Trgovina na malo i smještaj postižu visoke ocjene za zrelost interneta koja omogućuje komunikaciju s tržištem, dok su poduzeća u sektoru proizvodnje srednje i visoke tehnologije, poput onih iz IKT sektora i proizvodnje električne energije, uspješnije orijentirana na integraciju IKT aplikacija u poslovne procese.

2.1.2. Industrije: prihvaćanje digitalnih rješenja

Razina prihvaćanja digitalnih rješenja i tehnologija u poslovanju u različitim fazama lanca vrijednosti, također se razlikuje među industrijama. Prema podatcima istraživanja OECD-a (slika 2.) IKT sektor je vodeći u upotrebi svih rješenja, od korištenja računalnog oblaka do prodaje preko interneta.

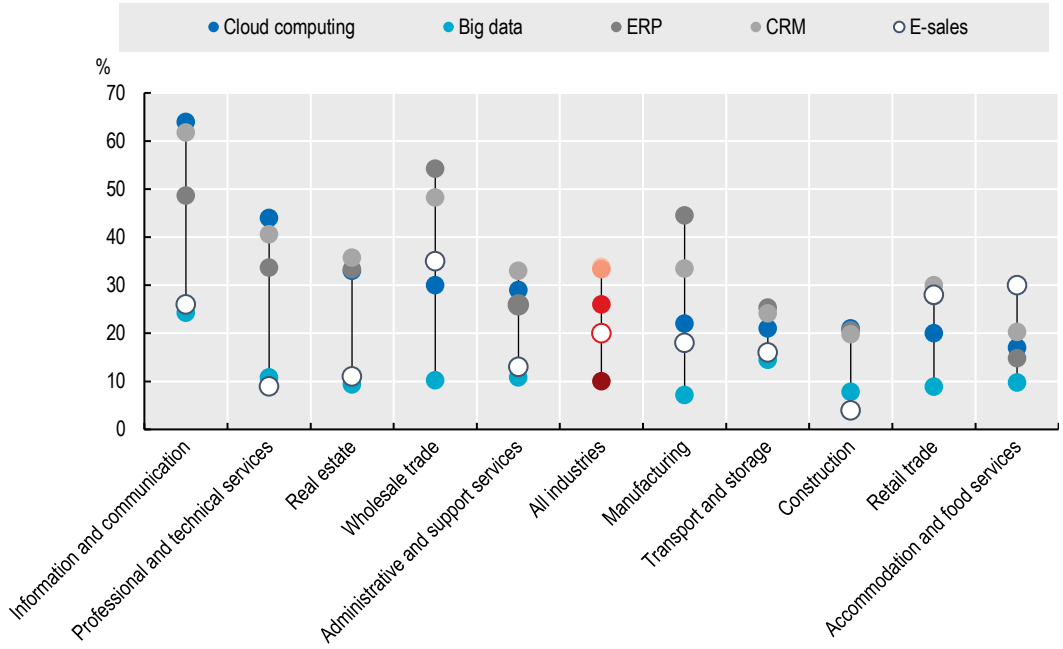
Industrije se najviše razlikuju u korištenju naprednih digitalnih rješenja, tako da računalni oblak koristi 65 % poduzeća iz IKT sektora te manje od 20 % poduzeća koja posluju u proizvodnom sektoru, transportu i skladištenju, građevinskom sektoru, maloprodaji i sektoru pružanja smještaja i usluga.

S druge strane, poduzeća u sektoru pružanja smještaja i usluga, uz veleprodaju i IKT poduzeća, jedna su od vodećih industrija u prihvaćanju prodaje putem interneta. ERP tehnologija u većem su postotku prihvatila poduzeća koja se bave veleprodajom i proizvodnjom (54 %, odnosno 45 %), dok je *CRM* zaživio u poduzećima iz sektora usluga, gdje ga je prihvatilo 41 % poduzeća (NACE L69-M74 Poslovanje nekretninama, Stručne, znanstvene i tehničke usluge). U ostalim industrijama, s iznimkom IKT-a, korištenje naprednih digitalnih rješenja poput *Big data*, ERP-a i CRM-a je na niskoj razini.

Za usporedbu, u Republici Hrvatskoj usluge računalnog oblaka je 2019. godini koristilo je 37 % poduzeća, što je porast od 6 % u odnosu na godinu prije. Uslugom se podjednako koriste mala, srednja i velika poduzeća, a vodeće industrije korisnici su IKT poduzeća (55 %) i trgovina (44 %) (DZS, 2019).

Slika 2. Korištenje IKT rješenja prema industrijama, zemlje EU, 2018.

% poduzeća s deset i više zaposlenih osoba u svakoj od industrija



Izvor: OECD (2019)

2.1.3. Industrije: digitalna transformacija u proizvodnji

Jedna od ključnih odrednica digitalne transformacije je uvođenje digitalizacije u proizvodnju. Korištenje naprednih tehnika kao što su *Big data*, 3D ispis, M2M komunikacija i robotizacije značajno mijenja proces proizvodnje. Usvajanje robotizacije u procese karakteristično je za Koreju i Japan u kojima je indeks zasićenosti prikazan kao broj robota po zaposleniku tri puta veći u odnosu na prosjek zemalja OECD-a (OECD, 2019).

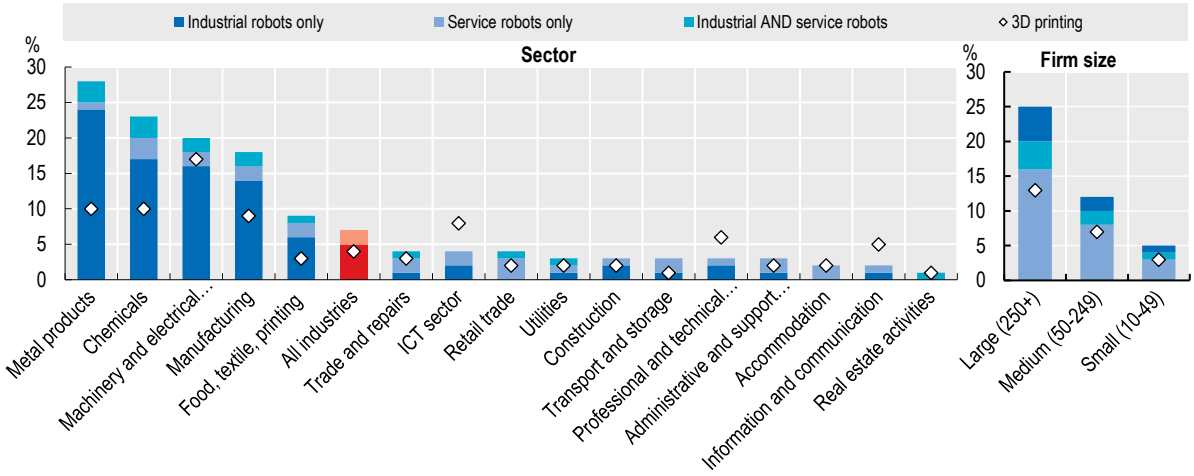
Prvi statistički podatci o upotrebi industrijskih i uslužnih robota i 3D ispisa u poduzećima u zemljama Europske Unije prikupljeni su u sklopu istraživanja Primjena informacijskih i komunikacijskih tehnologija (IKT) u poduzećima u 2018. godini. U prosjeku je 7 % poduzeća s više od deset zaposlenih koristilo robote, a 4 % koristilo je 3D ispis, s tim da je veća incidencija

poduzeća koje koriste ove tehnologije zabilježena u proizvodnji metalnih proizvoda, kemijskih proizvoda i strojeva (DZS, 2018).

Razlike se javljaju i s obzirom na veličinu poduzeća, i to u korist poduzeća s većim brojem zaposlenih. Tako je, primjerice, udio velikih tvrtki koje koriste industrijske ili uslužne robote 5 puta veći od udjela korištenja u malim tvrtkama. Korištenje 3D ispisa također je češće u velikim tvrtkama, s tim da je omjer postotka korisnika nešto manji, točnije postotak u većim tvrtkama je 4,3 puta viši u odnosu na male tvrtke.

Slika 3. Korištenje robotike i 3D ispisa u poduzećima, prema sektoru i veličini poduzeća, zemlje EU, 2018.

% poduzeća s deset i više zaposlenih osoba u svakoj od industrija



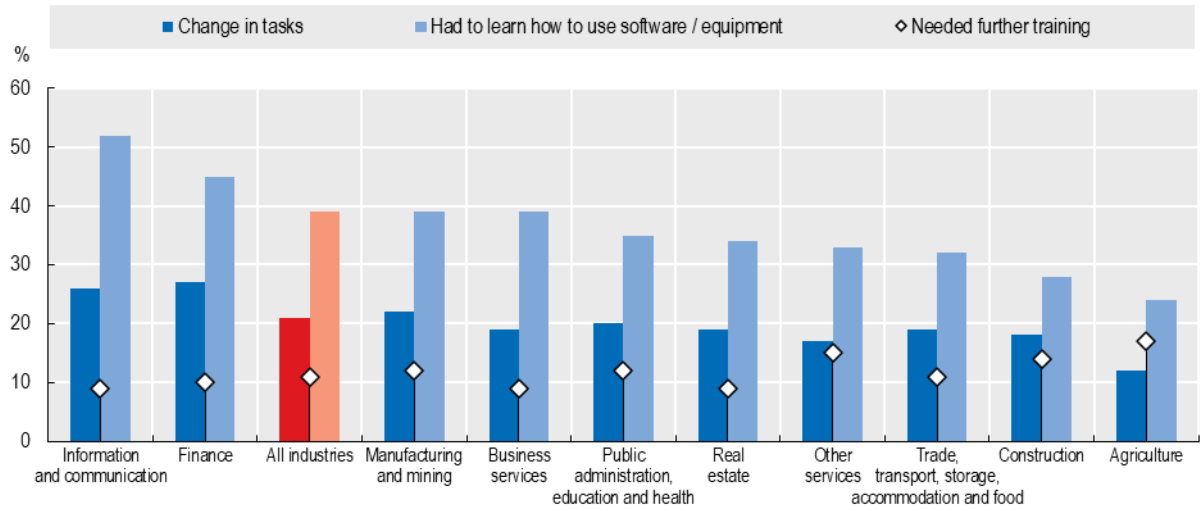
Izvor: OECD (2019)

2.1.4. Industrije: digitalna transformacija i zaposlenici

Podatak o tome da je u 2018. godini više od polovice zaposlenih u zemljama EU koristilo IKT tehnologije u svakodnevnom radu, najbolje ilustrira važnost i veličinu utjecaja digitalizacije u poduzećima. Uz broj zaposlenika koji koriste informatičke tehnologije, digitalna transformacija u poduzećima također podrazumijeva i usvajanje novih vještina i znanja, što nadalje zahtjeva više vremena i angažmana zaposlenika, te prilagodbu na nove uvjete i organizaciju rada. U 2018. godini je gotovo 40 % zaposlenika u EU moralo naučiti koristiti novi softver ili IKT alate. Učenje novih digitalnih alata potrebnih na radnom mjestu najizraženije je u IKT sektoru (52 % zaposlenih) i financijama (45 %), a najmanje je prisutno u poljoprivredi (24 %). Iako je u industriji poljoprivrede relativno najmanje onih koji su morali učiti kako koristiti nove softvere i opremu, postotak onih koji su trebali dodatnu edukaciju je najveći (17 % u odnosu na prosjek od 11 %).

Slika 4. Utjecaj novih softvera ili računalne opreme na rad, prema industrijama, zemlje EU, 2018.

*% poduzeća s deset i više zaposlenih osoba u svakoj od industrija (*OECD, 2019.)



Izvor: OECD (2019)

Promjene u radu uslijed digitalizacije zamijetilo je oko 21 % zaposlenika, s tim da su na vrhu ljestvice zaposleni u financijama (27 %) i IKT industriji (26 %). Zaposleni u ostalim uslugama i poljoprivredi su u najmanjem postotku zamijetili promjene u svojim radnim zadatcima (17 % i 12 %).

U prosjeku je najveći postotak zaposlenika koji koriste digitalne tehnologije u svakodnevnom radu zamijetio utjecaj digitalizacije na povećanje vremena provedenog u učenju, na lakoću suradnje s kolegama, na mogućnosti praćenja radnog učinka i na samostalnost u organizaciji posla (oko 20 % odgovora). Istovremeno, svaki deseti zaposlenik smatra da je digitalizacija utjecala na povećanje broja radnih sati izvan radnog vremena. Zanimljivo je da postotak zaposlenika koji smatraju da je digitalizacija povećala broj repetitivnih zadataka gotovo jednak postotku onih koji smatraju da ga je smanjila (smanjenje 17,2 % , povećanje 15,3 %).

Uz promjene u samom sadržaju rada i radnim procesima iz perspektive samih djelatnika, digitalizacija i automatizacija radnih procesa može imati značajan utjecaj i na troškove proizvodnje, a time i na cijenu proizvoda. Ova pojava redovito značajno utječe na lanac vrijednosti u proizvodnji.

Automatizacijom rad postaje manje važnim proizvodnim faktorom što potiče proizvođače da proizvodne pogone, koje su proteklih desetljeća premjestili u zemlje u razvoju, vrate u razvijene zemlje Europe i Sjeverne Amerike. Taj je proces već počeo, a osim automatizacijom potaknut je povećanjem cijene rada u zemljama u razvoju, željom za većom kvalitetom proizvoda te potrebom smanjivanja udaljenosti od glavnih tržišta kako bi se lakše komuniciralo s kupcima i skratilo vrijeme isporuke[11] (Eurofound, 2020). Dakako, uslijed digitalizacije i automatizacije, broj zaposlenika u proizvodnim pogonima koji su se vratili u razvijene zemlje znatno je manji i znatno više uključuje visokoobrazovane kadrove (Butković i Samardžija, 2019).

[11] Eurofound (2020). European Working Conditions Survey - Data visualisation. Dostupno na https://www.eurofound.europa.eu/data/european-working-conditions-survey, pristupljeno 19.11.2020.

2.2. DESI Indeks gospodarske i društvene digitalizacije (DESI 2020)

Europska komisija je 11. lipnja 2020. godine objavila Indeks gospodarske i društvene digitalizacije (DESI) za 2020. godinu (s napomenom da je u 28 država članica EU u sve dokumente do kraja 2020. godine uključeno i Ujedinjeno Kraljevstvo).

Kako se tvrdi u izvješću, ovogodišnji DESI pokazuje da postoji napredak u svim državama članicama i u svim ključnim područjima mjerenim u indeksu. Ove činjenice postaju sve važnije u kontekstu pandemije COVID-19 virusa tijekom koje se pokazala važnost digitalnih tehnologija u funkcioniranju cjelokupnog društva. Osim toga, pokazatelji DESI relevantni za oporavak, signaliziraju da bi države članice EU-a trebale pojačati napore na poboljšanju pokrivenosti mreža vrlo velikog kapaciteta, dodijeliti 5G spektar kako bi se omogućilo komercijalno pokretanje 5G usluga te dodatno raditi na poboljšanju digitalnih vještina građana i daljnjoj digitalizaciji poduzeća i javnog sektora.

U kontekstu plana oporavka za Europu, usvojenog 27. svibnja 2020., DESI će poslužiti za izradu analize za svaku od zemalja. Analiza će omogućiti državama članicama fokusiranje i prioritizaciju reformskih i investicijskih projekata te olakšati pristup Fondu za oporavak i otpornost. Fond će državama članicama osigurati sredstva, kako bi njihova gospodarstva bila otpornija, i osigurati kvalitetniju realizaciju ulaganja i reformi u skladu s ciljevima zelene i digitalne tranzicije EU-a. Inače ukupna vrijednost Fonda je 560 milijardi eura, a Hrvatska prema najavama može aplicirati za iznos od 10 milijardi eura. Iako Europska unija još uvijek nije finalizirala kriterije Fonda za oporavak i način njegova punjenja, za očekivati je postavljanje glavnih smjernica od strane države i motiviranje poduzetnika za izradu prijedloga projekata.

Mjesec dana prije proglašenja pandemije, u veljači 2020. godine, Europska je komisija iznijela svoju viziju digitalne transformacije u komunikaciji, Oblikovanje digitalne budućnosti Europe[12], kako bi omogućila uključivo korištenje tehnologije stanovništva i poštivanje temeljne vrijednosti EU-a. Bijela knjiga o umjetnoj inteligenciji (*The White Paper on Artificial*

[12] Europska komisija (2020). *Shaping Europe's digital future*. Dostupno na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en, pristupljeno 10.01.2021.

Intelligence) i europska podatkovna strategija (*The European Data Strategy*) prva su dva stupa nove digitalne strategije Komisije. Komisija je 10. ožujka 2020. godine objavila svoju novu strategiju za mala i srednja poduzeća[13] za održivu i digitalnu Europu. DESI će se koristiti za praćenje napretka u digitalizaciji malog i srednjeg poduzetništva na godišnjoj osnovi.

Nedugo nakon toga, svijet i sve članice EU našle su se pred izazovima pandemije COVID-19 virusa. Upravo je novonastala situacija dodatno naglasila važnost digitalizacije za funkcioniranje ekonomije te konkretnije ukazala kako mreže i povezanost, podatci, umjetna inteligencija (AI) kao i osnovne i napredne digitalne vještine utječu na ekonomiju i društvo omogućavajući održavanje nastave, praćenje širenje virusa i zajedničku potragu za lijekovima i cjepivima.

Na širenje utjecaja pandemije na gospodarstvo, Komisija je odgovorila pokretanjem nekoliko mjera na području digitalne tehnologije. Kao najvažnije, Komisija i Tijelo europskih regulatora elektroničkih komunikacija (BEREC) su 19. ožujka 2020. godine uspostavili poseban mehanizam izvještavanja za nadgledanje stanja internetskog prometa u svakoj državi članici kako bi mogli odgovoriti na pitanja vezana za kapacitet. Dana 25. ožujka 2020. godine pokrenuta je inicijativa za prikupljanje ideja o implementacijskim rješenjima AI i robotike, kao i informacija o drugim inicijativama koje bi mogle pomoći u reagiranju na pandemiju. Početkom travnja objavljena je preporuka za razvoj zajedničkog EU pristupa upotrebi mobilnih aplikacija i mobilnih podataka kao odgovora na pandemiju koronavirusa. Koalicija *Digital Skills and Jobs* započela je organizirati tematske *webinare* s Nacionalnim koalicijama i njihovim članovima kako bi podijelili svoje rješenja i iskustva kao odgovor na iznenadnu potrebu za digitalnim vještinama među Europljanima.

Prema izvješću iz 2020. godine, Hrvatska s ukupnim rezultatom od 47,6 % zauzima 20 mjesto od 28 država članica EU (s uključenim Ujedinjenim Kraljevstvom), što je rang jednak onome iz prošle godine i nešto bolji u usporedbi s rezultatom iz 2018. godine. Iz toga proizlazi i što za Hrvatsku znači biti na dvadesetom mjestu, po čemu smo točno dvadeseti, u kojim područjima je vidljiv napredak, tko nas je prestigao, a tko je iza nas.

[13] Europska komisija (2020). *SME Strategy: Internal Market, Industry, Entrepreneurship and SMEs*. Dostupno na: https://ec.europa.eu/growth/smes/sme-strategy_en, pristupljeno 10.01.2021.

Tablica 1. Indeks gospodarske i društvene digitalizacije RH i usporedba s Europskom unijom

	Hrvatska		EU
	rang	rezultat	rezultat
DESI 2020.	20	47,6	52,6
DESI 2019.	20	44,3	49,4
DESI 2018.	21	40,8	46,5

Izvor: Europska komisija (2020a)

DESI pokazatelj gospodarske i društvene digitalizacije sastoji se od pet tematskih pokazatelja i njihovih karakteristika[14]:

„1) Povezivost: Fiksni širokopojasni pristup, mobilni širokopojasni pristup i cijene

Pristup brzoj i pouzdanoj širokopojasnoj vezi (uključujući fiksne i mobilne veze) presudan je u trenutnom kontekstu u kojem se ključne društvene i ekonomske usluge pružaju putem interneta. Važnost ovog pokazatelja digitalizacije za gospodarstvo i sve građane pokazala se i tijekom krize uzrokovane Covid-19 virusom kada su se pružatelji usluga suočili sa znatno povećanom potražnjom i opterećenjem mreža.

2) Ljudski kapital: Upotreba interneta, osnovne i napredne digitalne vještine

Digitalne vještine predstavljaju stup digitalnog društva. Omogućuju ljudima korištenje digitalnih usluga i bavljenje osnovnim aktivnostima na mreži, što je od osobite važnosti u uvjetima ograničene mobilnosti. Digitalne vještine građanima omogućuju pristup informacijama i uslugama i sve više postaju nužne za svakodnevno funkcioniranje u društvu. Kao i element povezanosti, upotreba digitalnih vještina pokazala se ključnom tijekom pandemije za cijelo društvo, bilo za zdravstveno osoblje, državne službenike,

[14] Europska komisija (2020). *Digital Economy and Society Index (DESI) 2020*. Dostupno na: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1022m, pristupljeno 10.01.2021.

nastavnike/profesore i učenike/studente tako i za osobe koje su u riziku od socijalne isključenosti.

3) Upotreba internetskih usluga: Koliko se građani služe internetskim sadržajem i sudjeluju u komunikaciji ili transakcijama na internetu

Ova dimenzija DESI-ja mjeri koliko ljudi koristi internet i koje aktivnosti obavljaju na mreži. Bilježe se aktivnosti korištenja internetskog sadržaja (npr. slušanje glazbe, gledanje filmova, TV-a ili igranje igara, praćenje medija ili korištenje društvenih mreža), audio i video komunikacijske aktivnosti (npr. sudjelovanje u videopozivima) i financijske transakcije kao što su kupnja i bankarstvo preko interneta.

4) Integracija digitalne tehnologije: Digitalizacija poduzeća i e-trgovina

Ova dimenzija mjeri digitalizaciju poduzeća i e-trgovinu. Digitalne tehnologije predstavljaju konkurentsku prednost tvrtkama i omogućuju im unaprjeđenje procesa, poboljšavanje usluga i proizvoda i širenje na inozemna tržišta. Digitalna transformacija poduzeća otvara niz novih mogućnosti za tvrtke te potiče razvoj novih i pouzdanih tehnologija.

5) Digitalne javne usluge: e-uprava i e-zdravstvo

Ova dimenzija mjeri potražnju digitalnih javnih usluga kao i dostupnost baza podataka. Povećanje spektra digitalnih usluga i pogodnosti kroz uvođenje e-uprave omogućuje veću učinkovitost i uštede i za vlade i tvrtke. Također, uvođenje e-uprave redovito povećava transparentnost i otvorenost cjelokupnog društva.„

Ukupni DESI rezultat dobiva se kombiniranjem ponderirane prosječne vrijednosti svakog od navedenih pokazatelja i to na sljedeći način: 1. povezanost (25 %), 2. ljudski kapital (25 %), 3. korištenje interneta (15 %), 4. integracija digitalne tehnologije (20 %) i 5 digitalne javne usluge (15 %). Vrijednosti indeksa za svaki od pokazatelja/sastavnica i ukupna DESI vrijednost kreću se na skali od 0 do 100 što omogućava jednostavnu usporedbu između pojedinih sastavnica

indeksa, zatim usporedbu između različitih zemalja te usporedbu kretanja rezultata kroz vrijeme.[15]

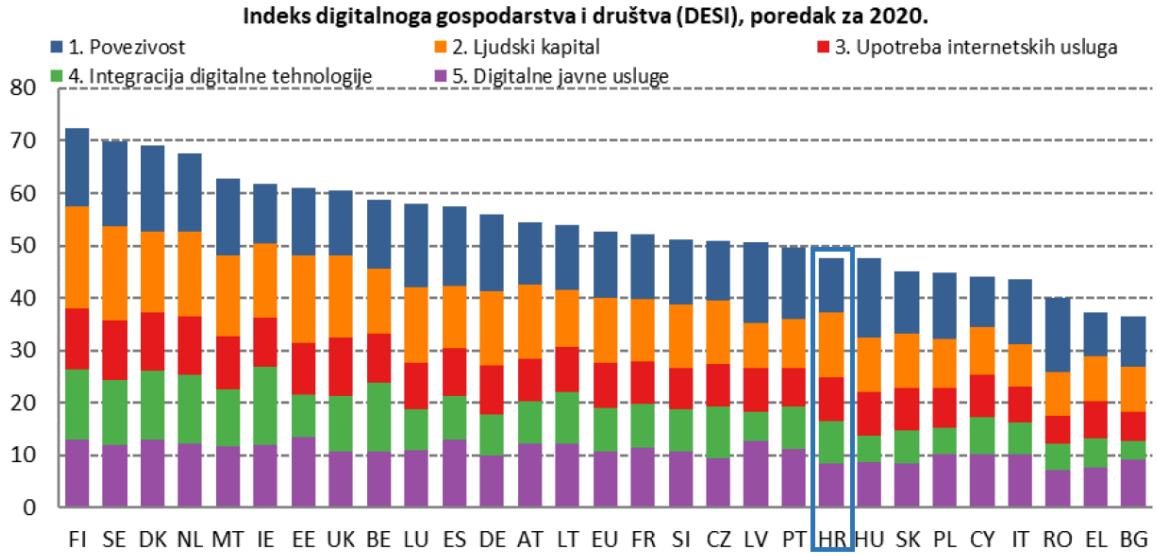
2.3. Hrvatska u usporedbi s ostalim zemljama EU

Prema ukupnom DESI rezultatu u 2020. godini Hrvatska se s 47,6 bodova nalazi na 20 mjestu, što je za pet postotnih bodova manje od prosjeka EU koji iznosi 52,6. Vodeće pozicije zauzimaju skandinavske zemlje, Finska sa 72,3, Švedska sa 69,7 i Danska sa 69,1 bodova, dok se na začelju ljestvice nalaze Grčka i Bugarska s manje od 40 bodova (Europska komisija, 2020a).

S obzirom na to da se Hrvatska posljednja pridružila EU zemljama, 20. mjesto prema indeksu digitalizacije nije loš rezultat u konkurenciji 28 država, osobito jer je Hrvatska u gotovo svim elementima indeksa ostvarila bolji rezultat u odnosu na prošlu godinu No vidljivo je zaostajanje u digitalizaciji javnog sektora (25. mjesto) i povezanosti (25. mjesto) te iznadprosječan rezultat na indeksu ljudskog kapitala (13. mjesto).

[15] European Comission (2020). *Digital Scoreboard: Digital Economy and Society Index*. Dostupno na: https://digital-agenda-data.eu/datasets/desi/indicators, pristupljeno 10.01.2021.

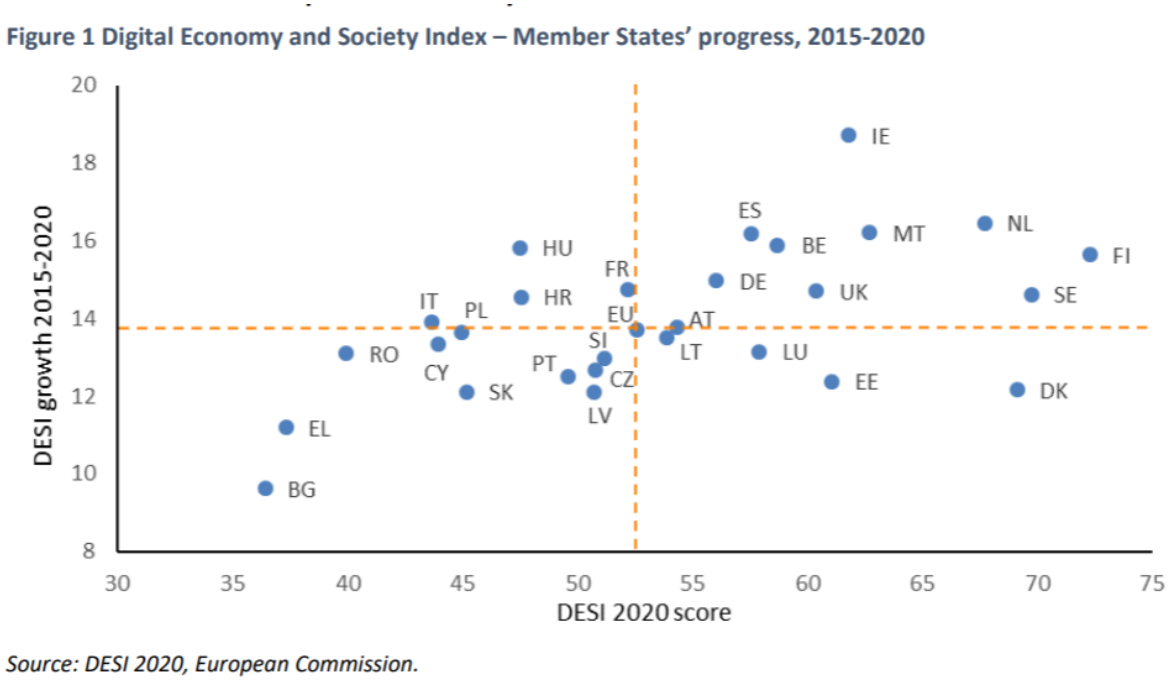
Slika 5. DESI 2020.



Izvor: Europska komisija (2020a)

Podatak o rangu prema ukupnom rezultatu za 2020. godinu sam po sebi ne govori previše o postignućima određene zemlje pa tako ni Hrvatske. Međutim, kada se ovogodišnji rezultat Hrvatske na DESI-ju od 47,6 stavi u kontekst ostalih zemalja EU-a i rezultata iz 2015. godine, otvara se mogućnost potpunije interpretacije. Hrvatska se, s obzirom na prosjek EU zemalja i rezultat iz 2015. godine, nalazi u skupini zemalja koje su ostvarile ispodprosječan ukupni rezultat u 2020. godini ali i iznadprosječan rast u odnosu na rezultat postignut 2015. godine (Slika 2.). Ovakva pozicija Hrvatske dopušta optimističan pogled u budućnost u kojoj se uz nastavak ulaganja u digitalnu infrastrukturu, edukaciju stanovništva i digitalnu transformaciju javnog i privatnog sektora, može nastaviti pozitivan trend i pridruživanje Hrvatske zemljama s iznadprosječnim DESI rezultatom. U sljedećem petogodišnjem razdoblju vjerojatno se ne može očekivati skok od gotovo 15 postotnih bodova ostvaren između 2015. i 2020. godine, ali se, uz jačanje pozitivnog trenda rasta, svakako može smanjiti zaostajanje za prosjekom EU-a. U ovom trenutku, u istoj skupini s Hrvatskom (gornji lijevi kvadrant na mapi) nalaze se i razvijenije članice EU-a, Italija, Mađarska i Francuska (Europska komisija, 2020b).

Slika 6. Odnos rasta indeksa gospodarske i društvene digitalizacije 2015. – 2020. i rezultata u 2020. godini.



Izvor: Europska komisija (2020b)

Povezivost

Na prvom od pet pokazatelja DESI indeksa, povezivosti, Hrvatska je ostvarila bolji rezultat u odnosu na 2019. godinu, ali je i dalje ostala na, ne tako dobroj, 25. poziciji. Razlog stagnacije su relativno niska potražnja za fiksnim širokopojasnim pristupom najmanje brzine 100 Mbps i izostanak sveobuhvatne strategije za uvođenje 5G mreže, koja je preduvjet za dodjelu koncesija.

Tablica 2. Povezivost, RH, rezultati 2018. – 2020. i usporedba s Europskom unijom, 2020.

POVEZIVOST	Hrvatska			EU
	DESI 2018.	DESI 2019.	DESI 2020.	DESI 2020.
1. Povezivost	32 %	37 %	41 %	50 %
1.a.1. Ukupna potražnja za fiksnim širokopojasnim pristupom % kućanstava	70 %	72 %	70 %	78 %
1.a.2 Potražnja za fiksnim širokopojasnim pristupom najmanje brzine 100 Mbps % kućanstava	1 %	5 %	6 %	26 %
1.b.1. Pokrivenost brzom širokopojasnom mrežom (nove generacije) % kućanstava	68 %	83 %	86 %	86 %
1.b.2. Pokrivenost fiksnom mrežom vrlo velikog kapaciteta % kućanstava	18 %	23 %	43 %	44 %
1.c.1. Pokrivenost mrežom 4G % kućanstava (prosjek operatora)	73 %	94 %	98 %	96 %
1.c.2. Potražnja za mobilnim širokopojasnim pristupom Broj pretplata na 100 stanovnika	82	85	89	100
1.c.3. Spremnost za 5G Dodijeljeni spektar kao % ukupnog usklađenog spektra za 5G	nije primjenjivo	0 %	0 %	21 %
1.d.1. Indeks cijena širokopojasnog pristupa	nije primjenjivo	nije primjenjivo	61	64

Izvor: Europska komisija (2020a), obrada autora

Ljudski kapital

Na pokazatelju ljudskog kapitala Hrvatska je na 13. mjestu, uz minimalnu razliku od jednog promila u odnosu na prosjek EU-a te uz napredak u odnosu na 2019. od 2,4 postotna boda. Područje u kojem Hrvatska ostvaruje najveću pozitivnu razliku u odnosu na prosjek je broj osoba s diplomom iz područja IKT-a koji trenutačno čine 5,5 % svih diplomiranih građana u Hrvatskoj. S druge strane, Hrvatska u odnosu na EU postiže niži rezultat u području posjedovanja digitalnih vještina stanovništva (56 % osoba u dobi od 16 do 74 godine ima

osnovne digitalne vještine, u odnosu na 61 % u EU). Međutim, u kategoriji digitalnih vještina na razini višoj od osnovne, Hrvatska je iznad prosjeka EU-a s rezultatom od 35 % (prosjek EU-a je 33 %).

Tablica 3. Ljudski kapital u indeksu gospodarske i društvene digitalizacije RH i usporedba s Europskom unijom

Ljudski kapital	Hrvatska		EU
	rang	Rezultat	rezultat
DESI 2020.	13	49,2	49,3
DESI 2019.	14	46,8	47,9
DESI 2018.	13	45,8	47,6

Izvor: Europska komisija (2020a), obrada autora

Upotreba internetskih usluga

Prema Schreckling i Steiger (2016), digitalne tehnologije izazvale su promjene u ponašanju ljudi, njihovim stavovima i očekivanjima, poglavito u brzini prihvaćanja novih tehnologija, a zatim i očekivanjima i komunikacije s onim što ih okružuje, planiranju aktivnosti i donošenju odluka te konačno dijeljenju iskustava i doživljaja s ostalima. Pritom je vidljivo da razvoj digitalnih rješenja i njihovo brzo prihvaćanje od strane krajnjih korisnika za sobom povlači i potrebu za izradom kvalitetnih rješenja, odnosno platformi i tehnologija za upravljanje i zaštitu njihovog digitalnog identiteta (Maliki i Seigneur, 2014).

Iako je napredovala u području upotrebe internetskih usluga u odnosu na prošlu godinu (55,5 u 2020. godini i 53,4 u 2019 godini), Hrvatska je pala na ljestvici zemalja EU-a s 14. na 15. mjesto. Hrvatski rezultati su relativno visoki u gotovo svim elementima korištenja internetskih usluga, a kod praćenja vijesti na internetu, slušanja glazbe, gledanja videa i igranja preko interneta te korištenja društvenih mreža i viši od europskog prosjeka. Lošiji rezultat Hrvatska

ima u području korištenja internet bankarstva (59 %, dok je prosjek EU-a 66%) i kupnju (57 %, dok je prosjek EU-a 71 %).

Tablica 4. Upotreba internetskih usluga u indeksu gospodarske i društvene digitalizacije RH i usporedba s EU

Upotreba internetskih usluga	Hrvatska		EU
	rang	rezultat	rezultat
DESI 2020.	15	55,5	58
DESI 2019.	14	53,4	55
DESI 2018.	17	49,2	51,8

Izvor: Europska komisija (2020a), obrada autora

Integracija digitalne tehnologije

Za tvrtke je nužno da budu usmjerene na mogućnosti i prepoznavanje problema u što ranijoj fazi. U uvjetima digitalnog poslovanja to mogu učiniti iskorištavanjem trendova u digitalizaciji čime mogu postići ne samo konkurentsku prednost kroz inovacije, nego se vrlo lako prilagoditi i izazovima poslovanja u uvjetima digitalne ekonomije (Kowalkiewicz et al 2016).

Značajan napredak u odnosu na prošlu godinu Hrvatska je ostvarila u području integracije digitalne tehnologije u poduzećima. Izjednačila se s prosjekom EU-a i zauzela 12. poziciju na ljestvici od 28 zemalja obuhvaćenih istraživanjem. Dobri rezultati postignuti su u trgovini putem interneta (21 % malih i srednjih poduzeća prodaje na internetu, 10 % prakticira prekograničnu prodaju na internetu u druge zemlje EU-a, a 22 % se koristi računalni oblak). Najveći pozitivni pomak u odnosu na 2019. ostvaren je u korištenju društvenih mreža (22 % aktivnih korisnika u 2020., 16 % u 2019.) Područje u kojem Hrvatska bilježi lošiji rezultat od europskog prosjeka i stagnira već tri godine, elektronička je razmjena informacija koju prakticira 26 % MSP-eva.

Tablica 5. Integracija digitalne tehnologije u indeksu gospodarske i društvene digitalizacije RH i usporedba s EU-om

Integracija digitalne tehnologije	Hrvatska		EU
	rang	rezultat	rezultat
DESI 2020.	12	41,5	41,4
DESI 2019.	17	38,5	39,8
DESI 2018.	16	36,7	37,8

Izvor: Europska komisija (2020a), obrada autora

Digitalne javne usluge

Hrvatska je postigla napredak u ukupnom rezultatu na području digitalizacije javnih usluga od pet postotnih bodova, ali i dalje zaostaje za europskim prosjekom koji iznosi 72 % i tako u konačnici zauzima ne tako dobro 25 mjesto. Jedini pokazatelj u kojem je ostvaren iznadprosječan rezultat su otvoreni podatci, dok u ostalim područjima, u područjima digitalnih javnih usluga za poduzeća i unaprijed ispunjenih obrazaca Hrvatska značajno zaostaje i stagnira.

Tablica 6. Digitalne javne usluge, rezultati 2018. - 2020. i usporedba s EU-om 2020.

DIGITALNE JAVNE USLUGE	**Hrvatska**			**EU**
	DESI 2018.	**DESI 2019.**	**DESI 2020.**	**DESI 2020.**
Digitalne javne usluge	**44 %**	**51 %**	**56 %**	**72 %**
5.a.1. Korisnici usluga e-uprave % internetskih korisnika koji trebaju podnijeti obrasce javnoj upravi	**66 %**	**75 %**	**65 %**	**67 %**
5.a.2. Unaprijed ispunjeni obrasci Bodovi (od 0 do 100)	**20**	**30**	**33**	**59**
5.a.3. Kompletnost usluga dostupnih na internetu Bodovi (od 0 do 100)	**62**	**64**	**73**	**90**
5.a.4. Digitalne javne usluge za poduzeća Bodovi (od 0 do 100) – uključujući domaće i prekogranične	**61**	**63**	**65**	**88**
5.a.5. Otvoreni podatci % maksimalnih bodova	**nije primjenjivo**	**nije primjenjivo**	**69 %**	**66 %**

Izvor: Europska komisija (2020a), obrada autora

2.4. Strategija EU 2020

Strategija EU 2020, formulirana je 2010. godine pod jakim utjecajem financijske krize koja se dogodila 2008. godine. Stoga ne čudi da je prva rečenica predgovora strategije kojeg je napisao tadašnji predsjednik Europske komisije Juan Manuel Barroso: „2010. mora označavati novi početak. Želim da Europa postane snažnija za ekonomsku i financijsku krizu“[16] (Europska komisija, 2011). Jedna od glavnih vodilja kod formuliranja strategije je potreba da Europska Unija, odnosno njezina članice što prije izađu iz krize, ali i da postanu otporne na buduće krize, a to će biti moguće samo kroz „pametan, održivi i uključiv razvoj“ zemalja članica.

Iz tih glavnih smjernica izvedeni su i osnovni indikatori praćenja razvoja za sve države članice EU-a. Eurostat kao vršna institucija u EU-u koja skuplja podatke iz država članica, objedinjuje ih i izvještava donositelje odluka (ali i zainteresiranu javnost), indikatore o praćenju strateških ciljeva podijelio je u pet skupina[17] (Eurostat, 2019b):

1. zaposlenost
2. istraživanje i razvoj (R&D) i inovacije
3. klimatske promjene i energija
4. obrazovanje
5. siromaštvo i socijalna isključenost.

Kako bi se osigurao i omogućio rast u svim strateški važnim područjima, Europska je komisija odredila sedam vodećih inicijativa. Jedna od tih inicijativa je Digitalna agenda za Europu (*Digital agenda for Europe*), čiji je cilj omogućavanje pristupa brzom (širokopojasnom) Internetu i stvaranje preduvjeta za iskorištavanje prednosti jedinstvenog digitalnog tržišta (DSM – *Digital Single Market*) kako za privatne osobe (kućanstva), tako i za poslovne korisnike.

[16] Europska komisija (2011). *Europe 2020: A European strategy for smart, sustainable and inclusive growth*. Dostupno na: https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf, pristupljeno 28.12.2020.

[17] Eurostat (2019b). *Smarter, greener, more inclusive? Indicators to support the Europe 2020 strategy*. 2019 Edition. Dostupno na: https://ec.europa.eu/eurostat/documents/3217494/10155585/KS-04-19-559-EN-N.pdf/b8528d01-4f4f-9c1e-4cd4-86c2328559de, pristupljeno 28.12.2020.

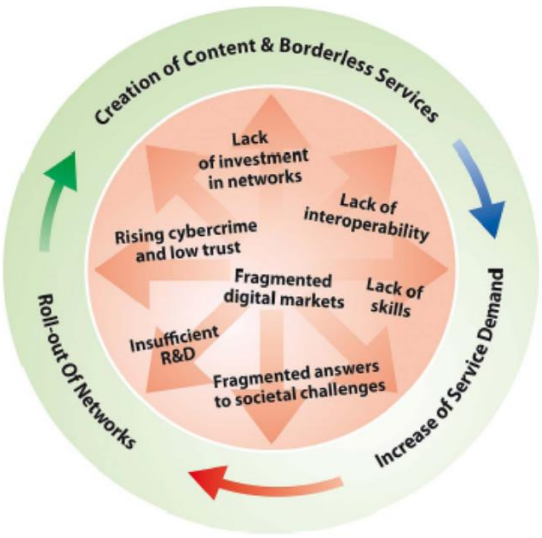
2.4.1. Digitalna Agenda za Europu (DAE) 2020

Digitalna agenda za Europu[18] (Europski parlament, 2020) prva je od sedam ključnih inicijativa predviđenih programom Strategije Europa 2020. Inicijativa je pokrenuta u svibnju 2010. godine, a cilj joj je omogućiti ekonomiji i građanima EU-a da ostvare maksimum korištenjem digitalnih tehnologija. DAE utvrđuje 101 mjeru grupiranu u sedam prioritetnih područja djelovanja na razini EU.

Digital Single Market (DSM) prvi je stup DAE koji sadrži 21 mjeru kojima se nastoji potaknuti promet internetskim sadržajem, uspostaviti jedinstveni okvir za internetsko plaćanje i omogućiti zaštita potrošača u digitalnom okruženju.

U prezenataciji DAE-a tadašnja je povjerenica Europske komisije za digitalnu agendu, Neelie Kroes[19] predstavila shematski okvir ciljeva digitalne agende za Europu 2020.

Slika 7. Shematski okvir ciljeva Digitalne agende za Europu 2020.



Izvor: Europska komisija (2011)

[18] Europski parlament. (2020). *Digital Agenda for Europe 2020*. Dostupno na: https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.3.pdf, pristupljeno 29.12.2020.
[19] Današnji naziv te funkcije je Izvršni potpredsjenik Europske komisije za Europu za Digitalno Doba i obnaša ju danska političarka Margrethe Vestager

Načini na koje će se ostvariti ciljevi digitalne agende grupirani su u sedam skupina:

- stvaranje jedinstvenoga digitalnog tržišta
- poboljšanje interoperativnosti informacijskih i komunikacijskih proizvoda i usluga (što uključuje i kreiranje boljih standarda i bolju uporabu standarda, te osiguravanje interoperabilnosti, čak i kada nema standarda)
- poticanje povjerenja i povećanje sigurnosti na internetu,
- osiguranje pružanja znatno bržeg pristupa internetu (slogan *Internet for all*)
- poticanje ulaganja u istraživanje i razvoj
- poboljšanje digitalne pismenosti, znanja i e-uključivosti
- razvoj i poboljšanje digitalnih javnih usluga – *eGovernment* usluge, *eHealth* usluge, međudržavne (*cross-border*) javne usluge za države članice.

Zbog utjecaja COVID-19 krize koja je uzdrmala Europu, kao i veliki dio svijeta, Europska je komisija objavila dokument o tome kako se COVID-19 kriza odrazila na ostvarivanje Digitalne agende[20] (Fipra International, 2020). Uslijed COVID krize došlo je do odgode donošenja zakonskih akata oko *E-Commerce* direktive[21], koja bi trebala biti uključena u budući *Digital Services Act (DSA)*[22], koji će biti u formi regulative, predložit će nova pravila za *online* platforme i osobito mjere za usklađivanje odgovornosti *online* platformi i pružatelja informacija te nadgledanje sadržaja na njima.

U digitalnoj strategiji Europska komisija jasno je izrazila namjeru redefiniranja pravila za digitalna tržišta. Uz to, namjera je i redefinirati tržište te su stoga nužne javne konzultacije, osobito oko definiranja „relevantnog tržišta proizvoda“ i „relevantnog geografskog tržišta“. Oko ova dva skupa ciljeva povezanih uz Digitalnu agendu, Europska komisija nije mijenjala rokove koji se uglavnom odnose na 2020. godinu.

[20] Fipra International (2020). *The EU'sDigital Agenda: in light of COVID-19*. Dostupno na: https://www.cabinet-samman.com/files/item/Digital%20look%20at%20the%20EU%20Digital%20agenda%20in%20light%20of%20COVID19%20-%2021%20April%202020.pdf, pristupljeno 15.12.2020.
[21] Europska komisija (2020). *E-Commerce directive*. Dostupno na: https://ec.europa.eu/digital-single-market/en/e-commerce-directive, pristupljeno 17.12.2020.
[22] Europska komisija (2020). *The Digital Services Act package*. Dostupno na: https://ec.europa.eu/digital-single-market/en/digital-services-act-package, pristupljeno 17.12.2020.

Do odgode je došlo i za donošenje regulative ili konzultacija vezanih uz pristup podatcima, izvještaj o evaluaciji učinka Uredbe te nekih regulativa vezanih uz *FinTech,* usluge odnosno financijske tehnologije.

Uz to je, u veljači ove godine Europska komisija objavila Digitalni paket[23] (*Digital Package)* kojim je postavila okvir u digitalnim područjima za sljedećih pet godina (Europska komisija, 2020c). Taj paket sadrži izlaganje o digitalnoj budućnosti Europe, strategiji vezanoj uz podatke i Bijelu knjigu[24] *(White Paper)* o umjetnoj inteligenciji.

U Digitalnom paketu nalaze se izložena četiri osnovna područja digitalne strategije EU za sljedećih pet godina[25]:

1. „**Tehnologija u službi čovjeka** – Razvoj, implementacija i primjena tehnologije koja pozitivno utječe na svakodnevni život ljudi. Snažno i konkurentno gospodarstvo koje upravlja tehnologijom i oblikuje ju u skladu s europskim vrijednostima.
2. **Pravedna i kompetitivna digitalna ekonomija** – Jedinstveno tržište bez suvišnih transakcijskih troškova, na kojem se tvrtke svih veličina i iz bilo kojeg područja mogu natjecati pod jednakim uvjetima, te mogu razvijati, plasirati i koristiti digitalne tehnologije, proizvode i usluge u mjeri koja povećava njihovu produktivnost i globalnu konkurentnost, a potrošači mogu biti sigurni da njihova se prava poštuju.
3. **Otvoreno, demokratsko i održivo digitalno društvo** – Pouzdano okruženje u kojem se građani osnažuju u načinu na koji djeluju i komuniciraju, kao i u podatcima koje pružaju na mreži i izvan nje. Europski način digitalne transformacije koji pojačava demokratske vrijednosti, poštuje naša temeljna prava i doprinosi održivom, klimatski neutralnom i učinkovitom gospodarstvu.
4. **Europa kao globalni digitalni čimbenik** – EU se zalaže za postavljanje globalnih standarda za nove tehnologije i ostat će najotvorenija regija za trgovinu i ulaganja na svijetu pod uvjetom da svatko tko ovdje posluje prihvaća i poštuje naša pravila.“

[23] Europska komisija (2020c). *Shaping Europe's digital future*. Dostupno na: https://ec.europa.eu/digital-single-market/en, pristupljeno 17.12.2020.
[24] Europska komisija (2020). *White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust*. Dostupno na: https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence, pristupljeno 10.09.2020.
[25] Europska komisija (2020). *The European Digital Strategy*. Dostupno na: https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy, pristupljeno 11.8.2020.

2.4.2. Europsko jedinstveno digitalno tržište (DSM)

Europsko jedinstveno digitalno tržište (DSM) jedno je od deset političkih prioriteta Europske komisije i predstavlja njezinu strategiju u dostizanju najboljeg mogućeg pristupa internetskom sadržaju i mogućnostima za pojedince i pravne subjekte. Glavna premisa DSM-a je osiguranje slobodnog kretanja osoba, usluga i kapitala u čijim *online* aktivnostima mogu sudjelovati pojedinci i pravni subjekti po uvjetima poštene konkurencije i visoke razine zaštite osobnih podataka, u svojstvu potrošača ili pojedinaca, bez obzira na njihovu nacionalnost ili mjesto prebivališta.

S obzirom na nove okolnosti digitalnog doba i digitalne transformacije sve većeg broja proizvoda i usluga, strategijom se želi osigurati da europsko gospodarstvo, industrija i društvo iskoriste potencijal globalnog širenja svojih mogućnosti i ukidanja regulatornih zapreka između zemalja članica Europske unije. Tijekom 2016. i 2017. godine uspješno su ukinute i naknade za *roaming*, modernizirana je zaštita podataka, postignuta je prekogranična prenosivost internetskog sadržaja te dogovor o uklanjanju prepreka e-trgovini ukidanjem neopravdanog geografskog blokiranja.[26] Trenutna procjena doprinosa funkcionalnog digitalnog tržišta gospodarstvu Europske unije iznosi i do 415 milijardi eura godišnje, a do 2025. godine bi digitalizacija proizvodnje mogla donijeti 1,25 bilijuna eura, čime bi Europska unija postala predvodnik u području svjetskih digitalnih postignuća.

Strategija DSM-a počiva na tri temelja: (1) pristup, (2) okolina te (3) gospodarstvo i društvo, odnosno bolji pristup potrošačima i pravnim subjektima prema digitalnim proizvodima i uslugama na području cijele Europe, omogućavanje jednakih uvjeta u svrhu nesmetanog napretka digitalnih mreža i inovativnih usluga te maksimiziranje potencijala rasta cjelokupne digitalne ekonomije.

Kod *online* plasmana svojih proizvoda i usluga, obveza je svih pravnih subjekata kao dionika na DSM-u i usklađenost sa svim zakonskim propisima te osiguravanje propisanih prava potrošačima.

[26] Europsko vijeće, Vijeće Europske unije (2020.) *Jedinstveno digitalno tržište za Europu*. Dostupno na https://www.consilium.europa.eu/hr/policies/digital-single-market/, pristupljeno 26.1.2020. godine.

2.4.3. Jedinstveno digitalno tržište iz perspektive potrošača

Uz sve koristi jedinstvenog digitalnog tržišta za poslovanje i za trgovinske razmjene između poslovnih subjekata, važno je istaknuti i konkretne koristi za krajnjeg potrošača.

Elektronička se kupnja se za krajnjeg potrošača često pretvara u vrlo neugodno iskustvo. Primjerice, mnoge mrežne trgovine (popularno zvani *web shopovi*) koriste geografsko blokiranje kupaca. Godine 2015. 63 % mrežnih trgovina u EU.u koristilo je takav način blokiranja kupaca iz drugih ili nekih država EU-a, a tek je 49 % mrežnih trgovina dostavljalo robu u državu kupca. Inicijative[27] povezane s Jedinstvenim digitalnim tržištem nastoje ukloniti takvu praksu i omogućiti da bilo koji građanin EU može kupovati proizvode iz bilo koje mrežne trgovine u EU-u neovisno o državi gdje se nalazi. Propisi doneseni 2018. godine sprječavaju diskriminaciju kupaca te će trgovci na internetu morati jednako postupati sa svim potrošačima u EU-u, odakle god oni odlučili kupovati.

Olakšavanje prekograničnog pristupa audiovizualnim uslugama također je dio inicijativa u okviru strategije jedinstvenog digitalnog tržišta. Prema Ekonomskoj studiji, o potrošačkim proizvodima s digitalnim sadržajem[28], svaki treći korisnik na internetu, što je ukupno 70 milijuna građana EU-a, susreo se s problemima povezanima s ugovornim pravom pri pristupu internetskom sadržaju, a samo je 10 % njih dobilo pravni lijek. Od travnja 2018. građani EU-a mogu svoje internetske pretplate na filmove, sportska događanja, e-knjige, videoigre ili glazbu upotrebljavati tijekom putovanja unutar EU-a.

Cijene prekogranične dostave paketa u prosjeku su bile 3 do 5 puta više od cijena domaće isporuke, bez jasnih razloga za tu razliku. Stoga su od svibnja 2018. godine bili na snazi propisi o internetskim uslugama prekogranične dostave paketa, čime se olakšava slanje paketa iz jedne države članice u drugu.

[27] Ibid.
[28] Europska komisija (2016). *Economic Study on Consumer Digital Content Products - Final Report*. Dostupno na: https://ec.europa.eu/info/sites/info/files/study-consumer-digital-content-products_en.pdf, pristupljeno 18.09.2020.

Od siječnja 2020. godine na snagu su stupili i novi propisi kojima se nacionalnim tijelima olakšava zaštita potrošača na internetu:

- stranice ili računi društvenih medija na kojima su otkrivene prijevare bit će uklonjene
- državne institucije mogu zatražiti informacije od pružatelja internetskih usluga ili banaka za utvrđivanje identiteta nepoštenih trgovaca na internetu
- europski centri i organizacije za zaštitu potrošača mogu slati obavijesti o lošim praksama.

U travnju 2018. godine Europska komisija predložila je *Nove pogodnosti za potrošače*[29], čime se povećavaju i prava potrošača na Internetu:

- internetske trgovine moraju potrošače obavijestiti o tome kupuju li od trgovca ili privatne osobe kako bi znali koja njihova prava ako nešto nije u redu
- pri pretraživanju na internetu jasno se mora pružati informacija o tome je li trgovac platio rezultat pretraživanja
- internetske trgovine moraju obavijestiti potrošače o glavnim parametrima za utvrđivanje rangiranja rezultata
- prilikom plaćanja digitalne usluge, potrošači imaju pravo na određene informacije i na rok od 14 dana za otkazivanje ugovora, a novim pogodnostima za potrošače to se pravo proširuje na „besplatne" digitalne usluge te se primjenjuje na to koliko dugo pružatelj usluga može koristiti podatke potrošača (npr. usluga pohrane podataka u oblaku, društveni mediji ili računi e-pošte).

Također, Europska je komisija predložila nove propise za digitalne ugovore koji bi jamčili jasna prava za potrošače kada pristupaju digitalnom sadržaju i digitalnim uslugama. Ta se prava odnose i na osobne podatke koje su potrošači dali trgovcima.

[29] Europski parlament (2020). *Četiri nove pogodnosti za potrošače*. Dostupno na: https://www.europarl.europa.eu/news/hr/headlines/economy/20190117STO23721/cetiri-nove-pogodnosti-za-potrosace, pristupljeno 17.09.2020.

2.5. E-Commerce

Digitalno poslovanje, odnosno digitalnu ekonomiju karakteriziraju (1) rastući broj mrežama međusobno povezanih ljudi, organizacija i strojeva i (2) korištenje digitalnih tehnologija i novih izvora podataka s digitalnih kanala, njihovog čuvanja u oblaku te analitike velikih podataka i korištenja mogućnosti umjetne inteligencije (Carvalho i Isaias 2019).

Jasno da većina definicija digitalne ekonomije kao obavezan element navodi tehnologiju koja ju omogućuje (Tugui, 2015; Strømmen-Bakhtiar, 2019; Daidj, 2019), međutim u nekima od definicija digitalne ekonomije naglašava se i njezin utjecaj na ostale sastavnice društva, primjerice kulturu. Primjer je definicija digitalne ekonomije kao sustava vezanih uz ekonomske, socijalne i kulturne odnose utemeljene na korištenju digitalnih kanala i tehnologija (Tolstykh et al., 2020). Referenca na kulturu je jasna budući da je kultura iskazana kroz dva međusobno povezana područja odnosno materijalnu i duhovnu kulturu koje zajedno predstavljaju od sredstava za proizvodnju i ostale materijalne tvorevine pa sve do ukupnosti rezultata znanosti, umjetnosti i filozofije, morala i običaja (Milanja, 2012).

Digitalne tehnologije pospješile su razvoj mnogih gospodarskih sektora kao i interakcija između pojedinaca općenito izazivajući pritom značajne pomake u ključnim industrijama i zahtijevajući od vodećih tvrtki brzu prilagodbu na nove tehnološke zahtjeve. (Kotler et al, 2017). Jedan od istaknutijih aspekata digitalnog poslovanja je elektronička trgovina koja omogućuje odvijanje transakcija roba i usluga putem interneta. Prema nekim autorima (Tolstoguzov i Pitukhina, 2020) glavnina digitalnog poslovanja odnosi se na e-trgovinu koja je usmjerena na proizvodnju digitalnih roba i usluga kao i da trgovci trebaju iskoračiti izvan sadašnjih granica kako bi se uskladili s novom erom digitalnog poslovanja, te da digitalizacija više nije izbor, već nužnost za sve trgovce koja podrazumijeva transformaciju poslovnih modela, uključivanje tehnoloških ulaganja, kao i tehnološko znanje (Seth i Wadhawan, 2016). Neki od autora razvoj e-trgovine smještaju u širi kontekst ostalih društvenih pokazatelja kao što su financijska pismenost, životni standard, priroda stanovanja, elektroničko plaćanje i ekonomija razmjera proizvodnih poduzeća (Wadhawan, i Arya, 2020).

Poduzećima koja uvode poslovni model elektroničke trgovine otvara se mogućnost korištenja učinkovitijih kanala distribucije i pristup većem broju kupaca što u konačnici dovodi do veće profitabilnosti poslovanja. S druge strane kupcima koji kupuju preko interneta osigurava se mogućnost izbora (Shahjee, 2016), mogućnost kupnje po povoljnijim cijenama kao i sigurnost kupnje. Važno je napomenuti da korištenje elektroničke trgovine značajno djeluje na minimiziranje sive ekonomije. Prema istraživanjima Međunarodnog monetarnog fonda (MMF), godišnje povećanje elektroničkog plaćanja od 10 % tijekom četiri uzastopne godine može smanjiti sivu ekonomiju do 5 % (Kelmanson et al, 2019). Jasno je da su elektroničko poslovanje i elektronička trgovina uz prednosti poput gospodarskog rasta i pojednostavljivanja poslovnih operacija, te smanjenja sive ekonomije doveli i do povećanja opasnosti od kibernetičkih napada (James, 2018).

Europski fond za regionalni razvoj u svom izvještaju o stanju e-trgovine u Europskoj uniji[30] razlikuje pet glavnih modela elektroničke trgovine s obzirom na to tko su strane koje sudjeluju u transakciji: pojedinci, tvrtke te državne institucije i javna poduzeća. Neki od autora navode i šesti model koji podrazumijeva transakcije između državnih tijela i građana (Valarmathy et al, 2018).

1. „**Elektronička trgovina na malo (B2C):** Transakcije u kojima tvrtke prodaju svoje proizvode ili usluge potrošačima (primjer kupnje televizora preko internetske trgovine)
2. **Elektronička trgovina između tvrtki (B2B):** Transakcije u kojima tvrtke prodaju svoje proizvode ili usluge drugim tvrtkama (npr. prodaja poslovne aplikacije drugoj tvrtki)
3. **Razmjena između pojedinaca (C2C):** Transakcije u kojima i kao kupci i kao prodavatelji sudjeluju krajnji potrošači. (primjer su različiti elektronički oglasnici, a najpoznatiji internacionalni primjer je *ebay*)
4. **Elektronička razmjena u kojoj pojedinci prodaju svoje proizvode ili usluge tvrtkama (C2B):** Primjer takve transakcije je situacija u tvrtka plaća *influenceru* objavu svojeg proizvoda ili usluge na njegovom profilu i na taj se način reklamira među njegovim pratiteljima.

[30] Europski fond za regionalni razvoj (2020). *Project Future Ecom: State of the Art Report E-Sales & Marketing*. Dostupno na: https://www.interregeurope.eu/fileadmin/user_upload/tx_tevprojects/library/file_1586338838.pdf, pristupljeno 23.8.2020.

5. **Tvrtke prema državi (B2G):** Transakcije u kojima tvrtke prodaju svoje proizvode ili usluge državi, državnim agencijama, lokalnoj upravi ili samoupravi. Primjer ovakve transakcije je prodaja konzultantskih usluga vezanih uz uvođenje novog softvera nekom gradu ili županiji.
6. ***Pojedinci prema državi (C2G):*** Transakcije između građana i javne uprave.„

U elektroničkim transakcijama, prema Hyderu (2020) najveću vrijednost imaju transakcije između tvrtki za koje se prema projekcijama za 2020. godinu smatra da će im vrijednost biti dvostruko veća od vrijednosti elektroničke trgovine na malo i koje predstavljaju najbrže rastući segment elektroničke trgovine u sljedećih pet godina. U elektroničkoj trgovini razlikuju se i vrste transakcija, koje je moguće podijeliti na prodaju preko mrežnih stranica i elektroničku razmjenu podataka (EDI). Elektronička razmjena podataka jedna je od najstarijih i najuspješnijih tehnologija koje se koriste u elektroničkim transakcijama između tvrtki, a definira se kao set standarda i protokola za razmjenu poslovnih transakcija u računalno razumljivom formatu.[31]

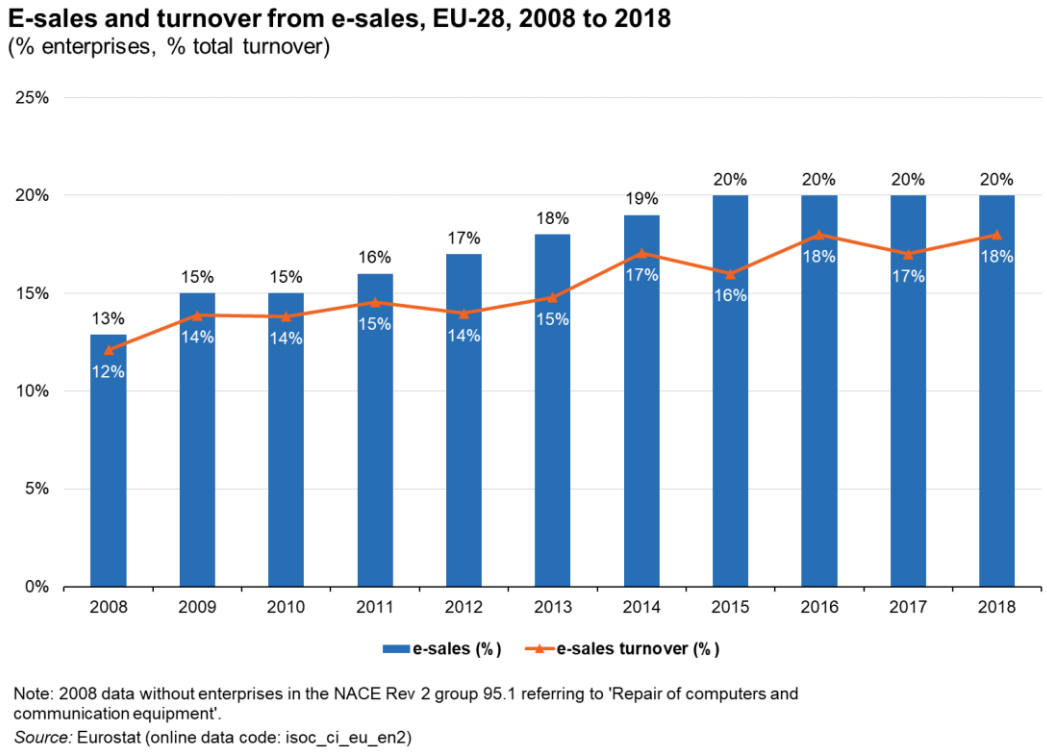
Dio koji slijedi, usmjeren je na statistiku elektroničke trgovine (e-trgovina) u Europskoj uniji, a temelji se na rezultatima istraživanja iz 2019. godine o Uporabi IKT-a i e-trgovini u poduzećima[32]. E-trgovina ovdje se odnosi na trgovinu robom ili uslugama putem računalnih mreža poput Interneta metodama posebno dizajniranim u svrhu primanja ili stavljanja narudžbi. Može se podijeliti na prodaju putem e-trgovine (e-prodaja) i kupnju putem e-trgovine (e-kupnja), ovisno o tome prima li poduzeće ili daje narudžbe.

U nastavku su prikazane detaljne informacije o elektroničkoj trgovini (e-trgovina) u 28 zemalja Europske unije koji temelje na rezultatima tog istraživanja. E-trgovina je u istraživanju definirana kao trgovina robom ili uslugama putem računalnih mreža metodama posebno

[31] Europski fond za regionalni razvoj (2020). *Project Future Ecom: State of the Art Report E-Sales & Marketing*. Dostupno na: https://www.interregeurope.eu/fileadmin/user_upload/tx_tevprojects/library/file_1586338838.pdf , pristupljeno 23.8.2020.
[32] Europska komisija (2020). Eurostat, *Statistics on ICT usage and e-commerce introduced*. Dostupno na: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_ICT_usage_and_e-commerce_introduced, pristupljeno 02.09.2020.

dizajniranim u svrhu primanja ili slanja narudžbi. Podatci u istraživanju odnose se na e-trgovinu tijekom 2018. godine, a podatci su prikupljeni za tvrtke s 10 i više zaposlenih.[33]

Slika 8. Udio tvrtki koje koriste elektroničku trgovinu i udio prometa ostvarenog elektroničkom trgovinom u ukupnom prometu, EU-28, 2008. –2018. (% tvrtki, % ukupnog prometa)



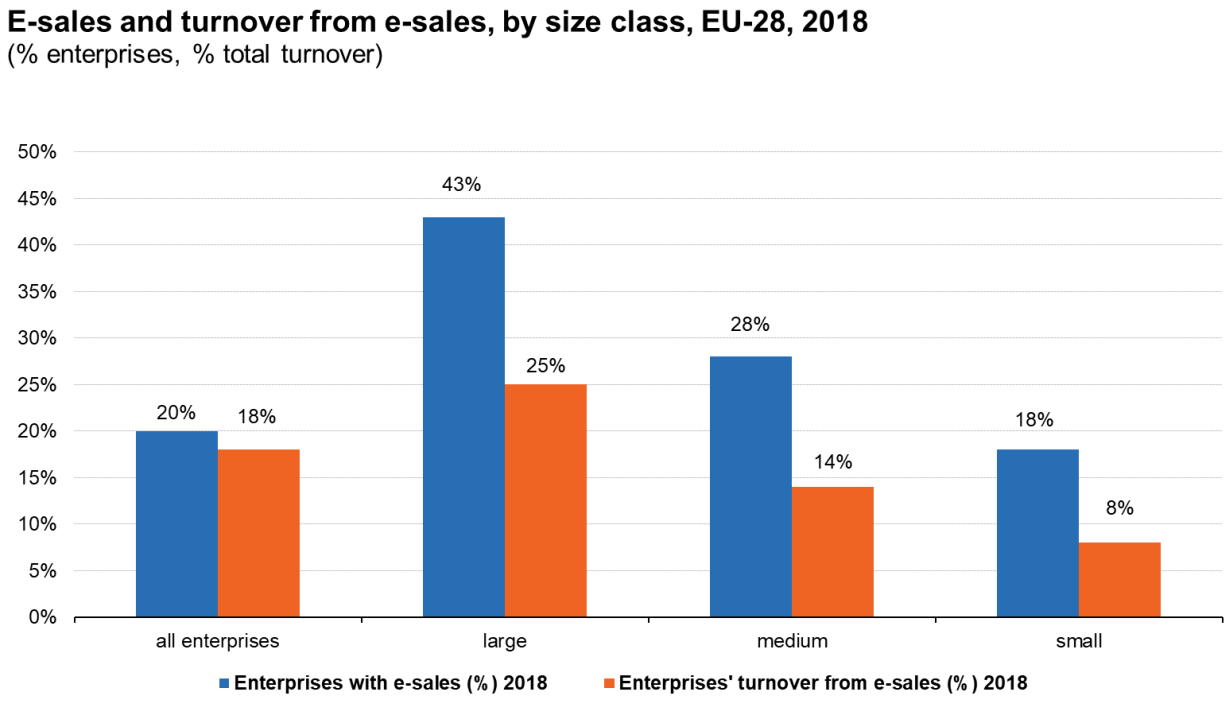
Izvor: Eurostat (2020)

U 2018. godini udio tvrtki koje koriste elektroničku trgovinu iznosio je 20 %, dok je udio prometa ostvarenog na takav način bio 18 %. Uočeno je da udio tvrtki koje koriste elektroničku trgovinu, stagnira već četiri godine uzastopno i zadržava se na 20 %. Ako se pogleda početak desetljeća, odnosno 2011. godina, vidi se da udio tvrtki s više od 10 zaposlenih koje koriste e-

[33] Europska komisija (2020). Eurostat, *E-commerce statistics*, Dostupno na: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics , pristupljeno 02.09.2020.

trgovinu, narastao je za 4 postotna boda, dok je udio prometa ostvarenog elektroničkom trgovinom povećan za 3 postotna boda, s 15 % na 18 %.

Slika 9. Udio tvrtki koje koriste elektroničku trgovinu i udio prometa ostvarenog elektroničkom trgovinom prema veličini tvrtke, EU-28, 2018 (% tvrtki, % ukupnog prometa)



Source: Eurostat (online data code: isoc_ci_eu_en2)

Izvor: Eurostat (2020)

Udio tvrtki koje koriste elektroničku trgovinu značajno varira s obzirom na njihovu veličinu, odnosno broj zaposlenih. Tako je 2018. godine udio tvrtki koje posluju koristeći e-trgovinu, kod manjih tvrtki iznosio 18 %, kod srednjih 28 %, a kod velikih 43 %. Posljedično, udio prometa ostvarenog e-trgovinom se kretao se od 8% u malim tvrtkama do 25 % u velikim tvrtkama.

Zanimljivo je promotriti podatke o elektroničkoj trgovini po zemljama Europe u 2018. godini. U sljedećoj tablici prikazan je udio tvrtki u kojima se odvija elektronička trgovina, s tim da su prikazani podatci i za zemlje izvan EU. [34]

Tablica 7. Udio tvrtki koje koriste elektroničku trgovinu prema zemljama, 2018.

Zemlja	Udio tvrtki %
EU-28 (uključujući UK)	20 %
Irska	39 %
Danska	34 %
Švedska	33 %
Belgija	31 %
Češka Republika	30 %
Finska	29 %
Nizozemska	27 %
Litva	26 %
Ujedinjeno Kraljevstvo	26 %
Slovenija	25 %
Austrija	24 %
Hrvatska	22 %
Estonija	21 %
Španjolska	21 %
Njemačka	20 %
Francuska	19 %
Portugal	17 %
Poljska	16 %
Mađarska	15 %
Slovačka	15 %
Italija	14 %
Cipar	14 %
Latvija	14 %
Luksemburg	14 %
Rumunjska	12 %
Bugarska	11 %
Grčka	11 %
Norveška	28 %

[34] Ibid.

Bosna i Hercegovina	21 %
Crna Gora	13 %
Turska	11 %
Malta	24 %
Island	:
Srbija	29 %
Sjeverna Makedonija	:

Izvor: Eurostat (2020)

Na vrhu ljestvice s udjelima od 30 % i više tvrtki koje koriste elektroničku trgovinu nalaze se Irska s 39 %, zatim Danska s 34 %, Švedska s 33 %, te Belgija s 31 % i Češka s 30 % .

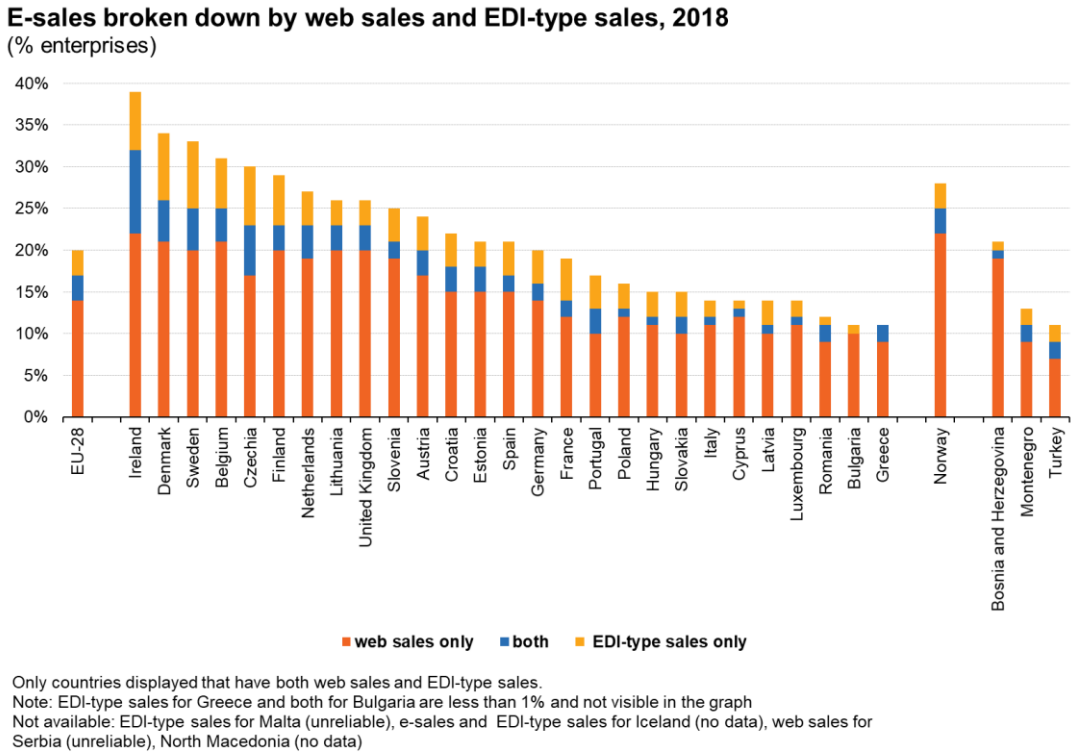
Hrvatska se s 22 % tvrtki nalazi u prvoj polovici ljestvice, iza Austrije i ispred Estonije. Zanimljivo je da u vodećim zemljama EU 28, Njemačkoj i Francuskoj e-trgovinu koristi postotno manji broj tvrtki nego u Hrvatskoj (20 % Njemačka i 19 % Francuska).

Osim navedene kategorizacije elektroničke trgovine s obzirom na sudionike transakcije (prodavatelja i kupca), elektroničku je trgovinu moguće promatrati s obzirom na to kako se odvija prodaja, odnosno novčana transakcija: preko mrežne stranice ili putem elektroničke razmjene podataka (EDI).[35]

Na grafičkom prikazu prezentirani su podatci samo za zemlje u kojima postoji elektronička razmjena podatka. Podatci su prikazani kao postotni udio tvrtki u određenoj zemlji koje koriste samo e-trgovinu preko mrežnih stranica, samo trgovinu preko elektroničke razmjene podataka ili oboje.

[35] Ibid.

Slika 10. Udio tvrtki koje koriste elektroničku trgovinu putem mrežnih stranica, elektroničkom razmjenom podataka (EDI) ili oboje, prema zemljama, EU-28, 2018 (% tvrtki)



Izvor: Eurostat (2020)

Na razini EU 28 dominira elektronička trgovina isključivo preko mrežnih stranica s 14 %, a podjednaki udio, točnije po 3 % tvrtki koristi elektroničku razmjenu podataka ili oba načina transakcija (i mrežne stranice i EDI). Sličan obrazac javlja se u svim zemljama, s izuzetkom Irske u kojoj je udio tvrtki koje podjednako koriste i elektroničku razmjenu podataka i mrežne stranice veći od onih koje koriste i isključivo elektroničku razmjenu podataka. Inače, kada se zbroje postotci tvrtki koje koriste elektroničku razmjenu podataka, isključivo ili u kombinaciji s transakcijama na mrežnim stranicama, na vrhu ljestvice je ponovno Irska sa 17 % tvrtki, praćena Danskom, Švedskom i Češkom u kojima EDI koristi 13 % tvrtki. U Hrvatskoj transakcije isključivo preko mrežnih stranica obavlja 15 % tvrtki, elektroničku razmjenu podataka koristi 4 % tvrtki, dok oba načina koristi 3 % tvrtki što je približno slično distribuciji

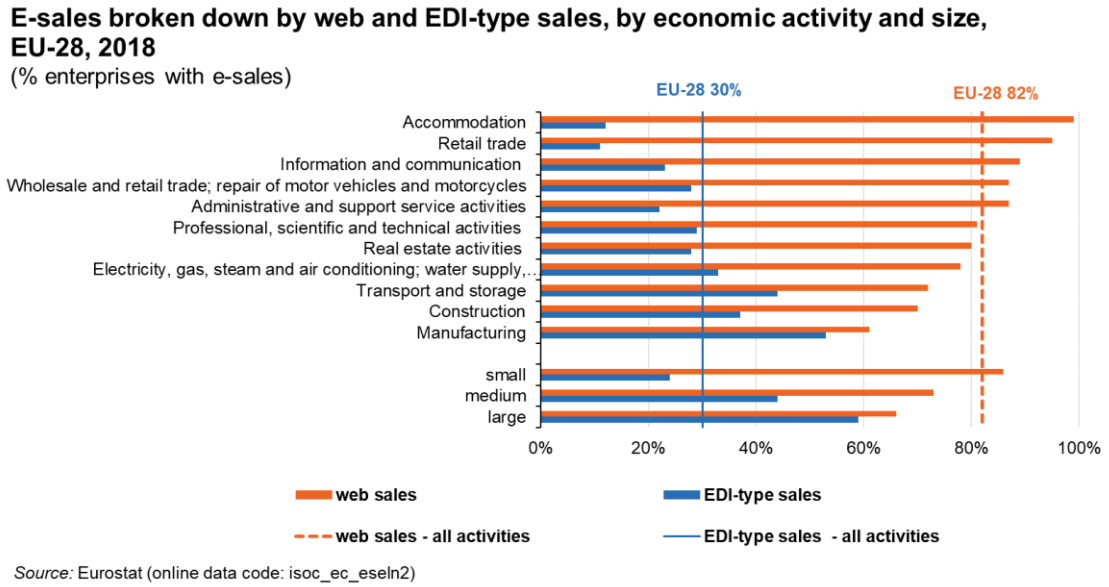
udjela načina plaćanja prosjeka EU 28. Načini obavljanja financijskih transakcija na području EU 28 znatno se razlikuju s obzirom na djelatnost u kojima tvrtke posluju i njihovu veličinu. [36]

Iako kod svih veličina tvrtki postotak tvrtki korisnika transakcija preko mrežnih stranica premašuje postotak tvrtki korisnika transakcija koje se odvijaju razmjenom elektroničkih podataka, razlika je daleko manja kod velikih tvrtki u odnosu na srednje i osobito male. Tako 66 % velikih tvrtki ostvaruje prodaju preko mrežnih stranica, a 59 % koristeći EDI; 73 % srednjih tvrtki za elektroničku trgovinu koristi mrežne stranice, dok ih 44 % koristi elektroničku razmjenu podataka. Kod malih tvrtki dominira trgovina preko mrežnih stranica koju koristi 86 % tvrtki, što je 3,6 puta više od udjela malih tvrtki koje koriste EDI.

Gledano prema industriji, elektronička trgovina preko mrežnih stranica se iznadprosječno koristi u sektorima smještaja, trgovini, IKT sektoru, veleprodaji i administrativnom sektoru. Elektronička je razmjena podataka u odnosu na prodaju preko mrežnih stranica manje prisutna u svima sektorima, ali je više od prosjeka koriste u sektorima proizvodnje, građevine, prijevoza i skladištenja te energetike, što je i u skladu s iznadprosječnim udjelom velikih tvrtki u ovim sektorima kao i prirode poslovanja (primjerice veća orijentacija na B2B trgovinu).

[36] Ibid.

Slika 11. Udio tvrtki koje koriste elektroničku trgovinu preko mrežnih stranica i elektroničkom razmjenom podataka (EDI) prema veličini tvrtke i industrijama, EU-28, 2018 (% tvrtki s e-trgovinom)



Izvor: Eurostat (2020)

Udio prometa ostvaren elektroničkom trgovinom u EU 28 zemljama varira od 4 % u Grčkoj do 34 % u Irskoj, a u prosjeku iznosi 18 % udjela u ukupnom prometu. Uz Irsku, kao vodeću zemlju prema kriteriju udjela prometa e-trgovine, u vrhu se nalaze Belgija s 33 % i Češka s 32 %.

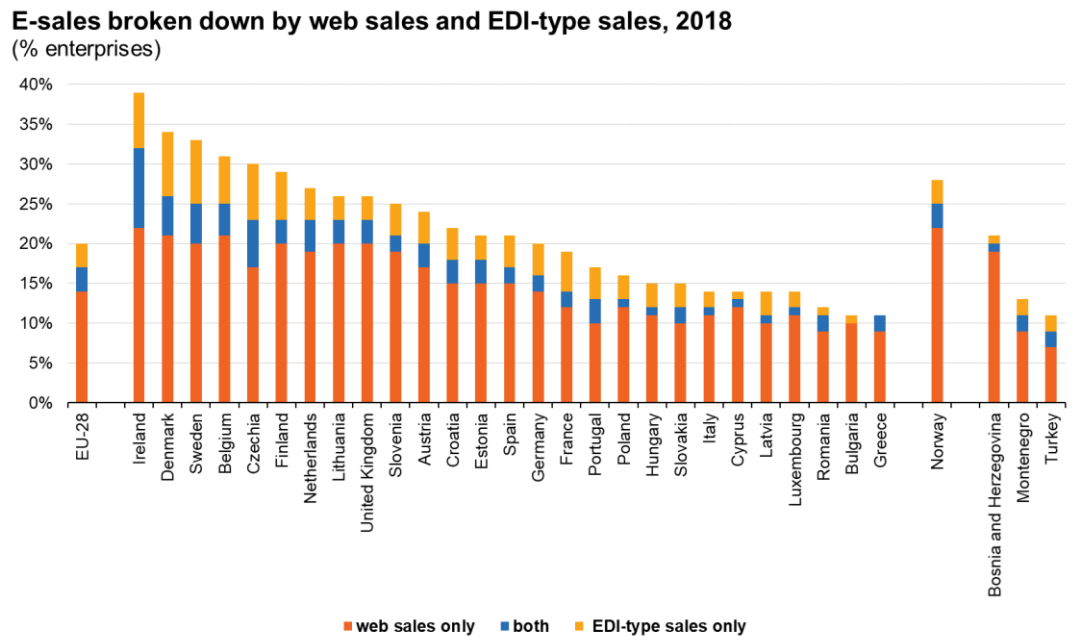
Hrvatska, s 11 % udjela prometa ostvarenog elektroničkom trgovinom u ukupnom prometu, zauzima dvadeseto mjesto na ljestvici.

Tablica 8. Udio prometa ostvarenog elektroničkom trgovinom u ukupnom prometu prema zemljama, 2018.

Zemlja	Udio prometa %
EU-28 (uključujući UK)	18 %
Irska	34 %
Belgija	33 %
Češka Republika	32 %
Danska	25 %
Švedska	25 %
Mađarska	23 %
Finska	23 %
Francuska	22 %
Ujedinjeno Kraljevstvo	21 %
Slovačka	21 %
Portugal	19 %
Poljska	18 %
Španjolska	18 %
Slovenija	17 %
Njemačka	15 %
Nizozemska	15 %
Estonija	14 %
Austrija	14 %
Litva	12 %
Hrvatska	11 %
Italija	11 %
Latvija	7 %
Rumunjska	7 %
Cipar	5 %
Bugarska	4 %
Grčka	4 %
Norveška	27 %
Srbija	15 %
Bosna i Hercegovina	11 %

Izvor: Eurostat (2020)

Slika 12. Udio tvrtki koje koriste elektroničku trgovinu preko mrežnih stranica i elektroničkom razmjenom podataka (EDI) prema zemljama, 2018 (% tvrtki)



Izvor: Eurostat (2020)

U većini zemalja udio prometa u e-trgovini ostvaren elektroničkom razmjenom podataka nadvisuje udio prometa ostvarenih putem mrežnih stranica. Iznimka su Velika Britanija, Nizozemska, Litva, Cipar i Grčka. U Hrvatskoj se udio prometa ostvarenog e-trgovinom raspoređuje na 6 % prometa ostvarenog elektroničkom razmjenom podataka i 5 % prometa ostvarenog preko mrežnih stranica, dok u Bosni i Hercegovini kao i u Srbiji, većina prometa ostvarenog e-trgovinom otpada na transakcije preko mrežnih stranica.

Udio prometa ostvarenom e-trgovinom preko mrežnih stranica i elektroničkom razmjenom podataka ovisi i o veličini tvrtke. U malim tvrtkama udio ostvaren preko mrežnih stranica, veći je od udjela u prometu ostvarenog elektroničkom razmjenom, (4 % i 3 %). Za razliku od malih tvrtki, u srednjim te, osobito, u velikim tvrtkama udio prometa ostvaren elektroničkom razmjenom podataka premašuje udio koji je ostvaren preko mrežnih stranica.

Osim s veličinom tvrtke, udio prometa ostvarenog e-trgovinom preko mrežnih stranica i elektroničkom razmjenom, povezan je i s industrijom. Najveći udio prometa ostvarenog elektroničkom razmjenom podataka bilježe industrije u područjima proizvodnje, energetike, te prometa i skladištenja (više od 10 %). Najveći udio prometa u e-trgovini ostvaren putem mrežnih stranica karakterističan je za usluge smještaja i iznosi visokih 28 %, što je četiri puta više od prosječnog udjela prometa u e-trgovini putem mrežnih stranica u zemljama EU 28.

Tablica 9. Udio prometa ostvarenog putem mrežnih stranica i prometa ostvarenog elektroničkom razmjenom podataka u ukupnom prometu (EDI) prema veličini tvrtke i industrijama, EU-28, 2018

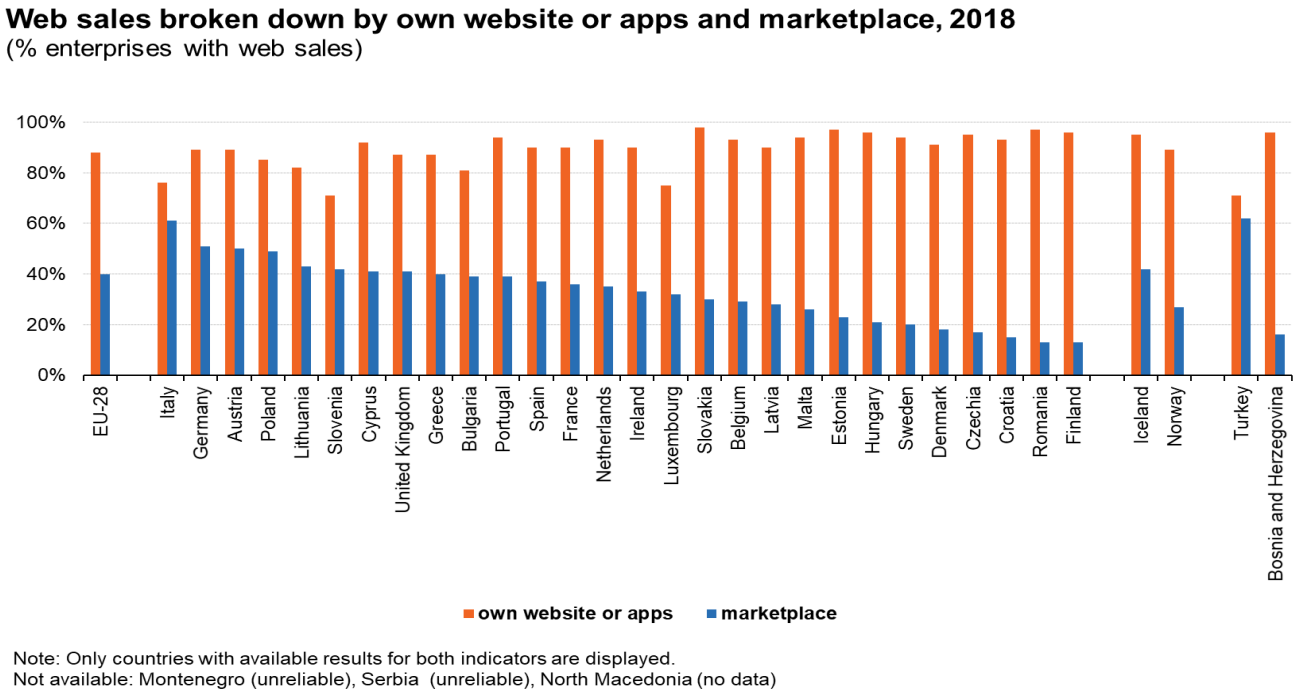
% prometa	Promet preko mrežnih stranica	Promet preko elektroničke razmjene podataka
EU-28 (uključujući UK)	7 %	11 %
Mali	4 %	3 %
Srednji	6 %	9 %
Veliki	9 %	16 %
Graditeljstvo	1 %	2 %
Stručne, znanstvene i tehničke djelatnosti	3 %	3 %
Poslovanje nekretninama	3 %	1 %
Proizvodnja	4 %	19 %
Trgovina na veliko i malo; popravak motornih vozila i motocikala	8 %	9 %
Trgovina na malo	8 %	2 %
Administrativne i pomoćne uslužne djelatnosti	9 %	3 %
Opskrba električnom energijom, plinom, parom i klimatizacija; opskrba vodom; uklanjanje otpadnih voda, gospodarenje otpadom te djelatnosti sanacije okoliša	9 %	12 %
Prijevoz i skladištenje	12 %	11 %
Informacijske i komunikacijske djelatnosti	14 %	5 %
Pružanje usluga smještaja	28 %	4 %

Izvor: Eurostat (2020)

Većina tvrtki koje prodaju preko mrežnih stranica, radi to preko vlastitih stranica ili aplikacija (88 %), dok se na prodaju preko elektroničkih stranica partnera odlučuje njih 40 % (zbroj nije 100 % jer neke od tvrtki koriste oba kanala prodaje). Od zemalja u EU 28 najveći udio tvrtki

koje prodaju preko stranica treće strane ima Italija i to 61 %, dok je Hrvatska zajedno s Rumunjskom i Finskom na dnu ljestvice s 15 % udjela tvrtki koje prodaju preko mrežnih stranica partnera (Slika 12).

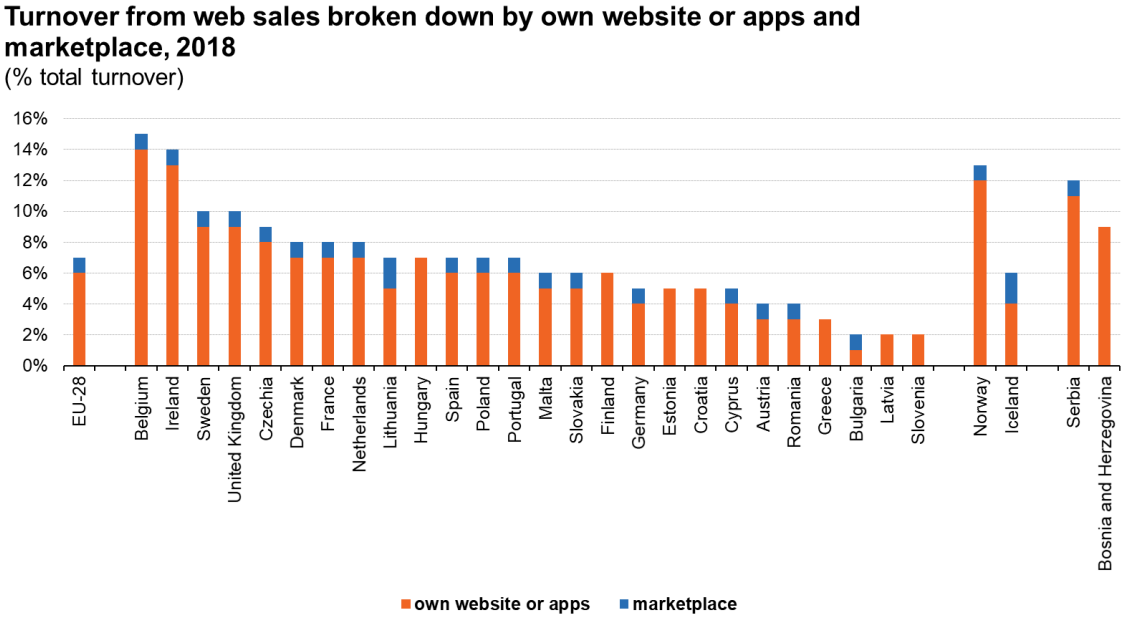
Slika 13. Prodaja preko mrežnih stranica, udio tvrtki prema prodaji preko vlastitih mrežnih stranica ili aplikacija i treće strane, 2018 (% tvrtki koje prodaju preko mrežnih stranica)



Note: Only countries with available results for both indicators are displayed.
Not available: Montenegro (unreliable), Serbia (unreliable), North Macedonia (no data)

Izvor: Eurostat (2020)

Slika 14. Udio prometa e-trgovine preko mrežnih stranica, udio u ukupnom prometu prema prodaji preko vlastitih mrežnih stranica ili aplikacija i preko treće strane, 2018 (% prometa)

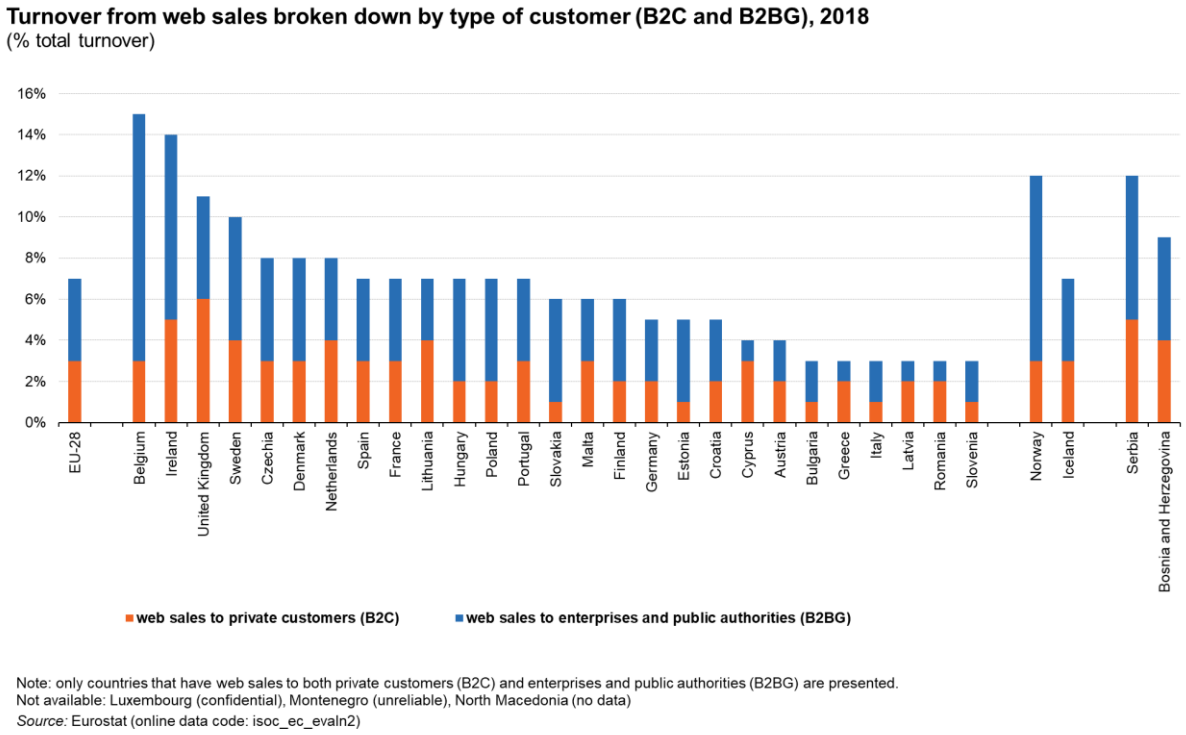


Note: Only countries with available results for both indicators are displayed.
Web sales via marketplace for Hungary, Finland, Estonia, Croatia, Greece, Latvia, Slovenia and Bosnia and Herzegovina are less than 1% and not visible in the graph
Not available: Luxembourg (confidential), Italy (unreliable), Montenegro (unreliable), North Macedonia (no data)

Izvor: Eurostat (2020)

Promet ostvaren prodajom preko mrežnih stranica u EU 28 zemljama iznosi 7 % ukupno ostvarenog prometa, od čega se 6 % ostvaruje putem prodaje preko vlastitih a tek 1 % preko stranica partnera. Sve zemlje za koje postoje podatci, osim Litve i Islanda kod kojih je udio prometa ostvarenog preko mrežnih stranica partnera 2 %, na ovaj način ostvaruju 1 % ili manje prometa. (Slika 14).

Slika 15. Udio prometa e-trgovine preko mrežnih stranica u ukupnom prometu prema vrsti kupca, udio u ukupnom prometu e- trgovine na malo (B2C) i e-trgovine između tvrtki i tvrtki s državom (B2B i B2G), 2018 (% prometa)



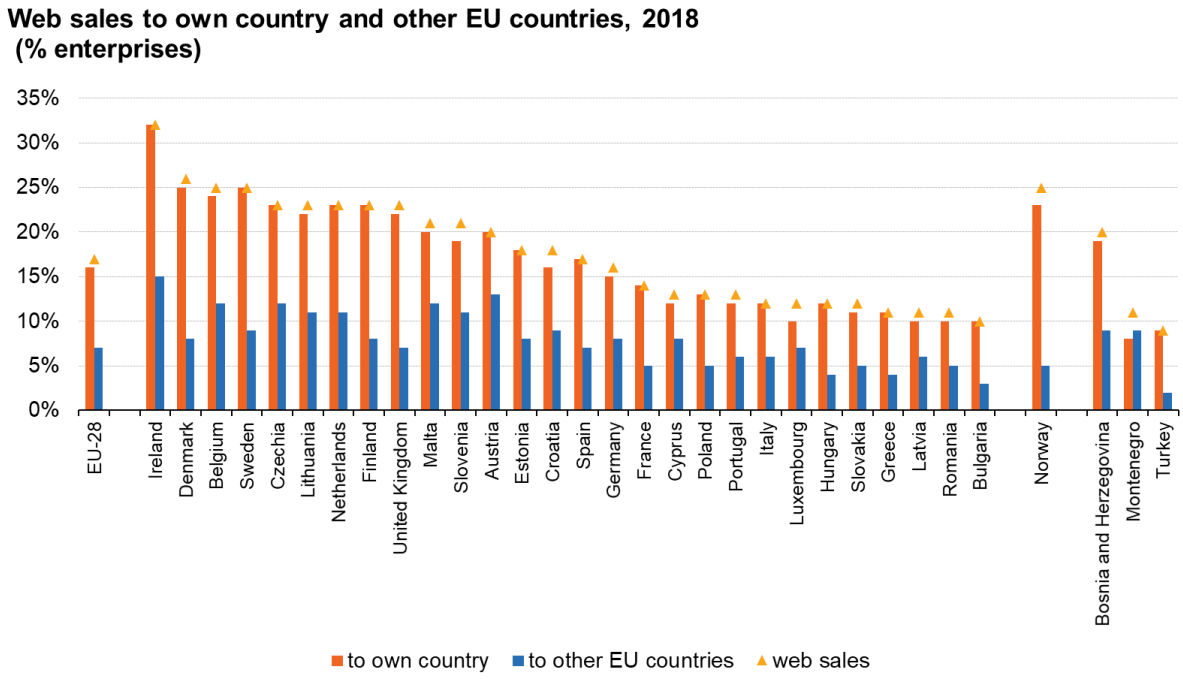
Note: only countries that have web sales to both private customers (B2C) and enterprises and public authorities (B2BG) are presented.
Not available: Luxembourg (confidential), Montenegro (unreliable), North Macedonia (no data)
Source: Eurostat (online data code: isoc_ec_evaln2)

Izvor: Eurostat (2020)

U zemljama EU 28 od 7 % udjela e-trgovine preko mrežnih stranica 3 % odnosi se na B2C ili trgovinu na malo, a 4 % na trgovinu među tvrtkama i trgovinu tvrtki prema državi (B2B i B2G). U samo pet zemalja promet ostvaren preko mrežnih stranica u e-trgovini na malo ima veći udio od prometa s državom i drugim tvrtkama, i to u Litvi, Cipru, Grčkoj, Latviji i Rumunjskoj.

Udio prometa ostvarenog e-trgovinom s poslovnim subjektima i državom najveći je u Belgiji i iznosi 12 %, a najmanji u Sloveniji, 3 %. Hrvatske tvrtke ostvaruju 5 % prometa u e-trgovini preko mrežnih stranica, od čega 2 % e-trgovini na malo i 3 % u e-trgovini s ostalim tvrtkama i s državom. Od europskih zemalja izvan EU-a, najveći udio B2B prometa u elektroničkoj prodaji imaju Norveška i Srbija (12 %).

Slika 16. Elektronička trgovina preko mrežnih stranica unutar zemlje i prema ostalim zemljama Europske unije, 2018 (% tvrtki)



Not available: Iceland (no data), web sales for Serbia (unreliable), North Macedonia (no data)
Source: Eurostat (online data code: isoc_ec_eseln2)

Izvor: Eurostat (2020)

U prosjeku 17 % tvrtki u Europskoj uniji prodaje preko mrežnih stranica, 16 % prodaje unutar vlastite zemlje, a 7 % u ostalim zemljama EU-a. Među EU zemljama s iznadprosječnim udjelom tvrtki koje preko mrežnih stranica prodaju u ostalim zemljama Unije, vodeća je Irska s 15 %, slijedi Austrija s 13 %, a zatim Belgija, Češka i Malta s udjelom od 12 % tvrtki koje preko mrežnih stranica prodaju u ostale zemlje EU-a. Hrvatska je s udjelom od 9 % tvrtki koje preko mrežnih stranica prodaju u ostale zemlje EU također iznad prosjeka prema ovom kriteriju.

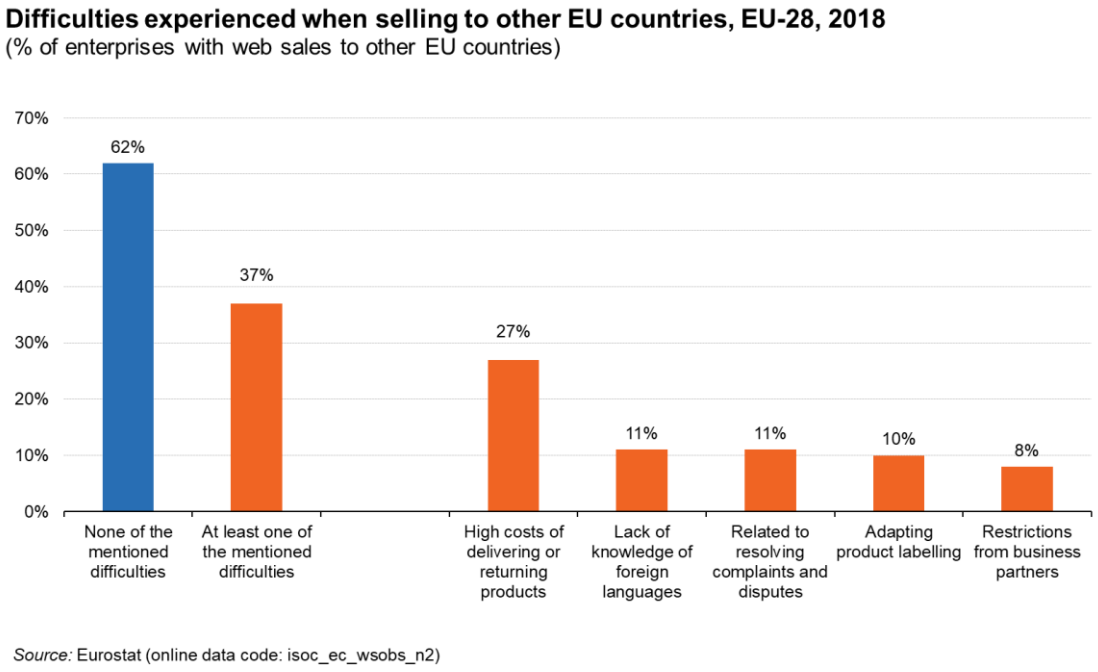
Zaključno o elektroničkoj trgovini

U razdoblju od 2015. do 2018. udio tvrtki unutar EU zemalja koje sudjeluju u e-trgovini stagnira na 20 %, dok se udio ostvarenog prometa kreće od 16 % do 18 %: u istom razdoblju. Većina e-trgovine odvija se preko mrežnih stranica, dok samo 6 % tvrtki koristi elektroničku razmjenu podataka. Elektronička razmjena podatka daleko je češća u velikim tvrtkama i u industrijama proizvodnje, prijevoza i skladištenja te građevinarstva, dok je prodaja preko mrežnih stranica karakteristična za tvrtke koje se bave uslugom smještaja.

Vodeće zemlje prema broju tvrtki koje se bave e-trgovinom kao i prema prihodima koje ostvaruju na taj način, su Irska, Belgija, Češka, Danska i Švedska.

Hrvatska s 22 % tvrtki koje sudjeluju u e-trgovini ima natprosječni rezultat, ali podatak o 11 % udjela e-trgovine u ukupnim prihodima ukazuje na to da postoji prostor za poboljšanje s obzirom na to da je riječ o relativno niskom vrijednosnom udjelu u ukupnom prihodu tvrtki. Prema ovom kriteriju Hrvatska je tek dvadeseta na ljestvici od 28 EU zemalja u 2018. godini. Možda je pozitivan pomak moguć i rješavanjem poteškoća koje navodi dio tvrtki (cijene dostave, nepoznavanje jezika, označavanje proizvoda).

Slika 17. Poteškoće u prodaji u ostale zemlje Europske unije, EU 28 2018 (postotak tvrtki koje prodaju preko mrežnih stranica u ostale zemlje Europske unije)



Izvor: Eurostat (2020)

Većina tvrtki u EU 28 ne nailazi ni na kakve poteškoće kod prodaje u ostale zemlje Europske unije, a njih 37 % navodi barem jednu prepreku. Prepreka koju navodi najviše tvrtki, je visoka cijena dostave ili povrata proizvoda (27 % tvrtki), dok nedostatke poput nepoznavanja stranih jezika, rješavanja pritužbi i prilagodbe oznaka na proizvodima, navodi svaka deseta tvrtka. Najmanje tvrtki navodi problem s ograničenjima koje im nameću poslovni partneri (8 %).

Uz problematiku, vezanu uz prodaju na internetu, koja je uočena u provedenom istraživanju, važno je ukazati i na sigurnosne probleme. Kod svakog ubrzanog razvoja pa tako i kod popularizacije korištenja digitalnih transakcija u elektroničkoj trgovini potrebno je pripremiti se za sigurnosne izazove (Thapa, 2018) i steći odgovarajuće znanje i razumijevanje pravnog okvira i mogućeg upravljanja problemima i rizicima (Shettar, 2016), a da bi se izbjegli sigurnosni problemi i osigurao operativni oporavak nastao uslijed eventualnih sigurnosnih propusta nužno je obrazovanje krajnjih korisnika, mrežna sigurnost i informacijska sigurnost te

uključivanje ostalih preventivnih radnji kao što su kontrole pristupa korisničkom računu, korištenje vatrozida i sustava za otkrivanje upada (Salkin i suradnici, 2018).

3. ISO standardi

Međunarodna organizacija za standardizaciju (*International Organization for Standardization - ISO*) međunarodno je tijelo za donošenje standarda, odnosno normi, sastavljeno od predstavnika raznih nacionalnih normizacijskih tijela. Kako bi se izbjeglo vezivanje uz bilo koji od svjetskih jezika te i po tom pitanju osigurala nepristranost, dogovoreno je da će se koristiti kratica ISO nastala od grčke riječi *isos*, što znači jednak. Osnovana 23. veljače 1947. godine, organizacija objavljuje industrijske i komercijalne norme. Iako je ISO nevladina organizacija, njegova sposobnost donošenja normi koje često postanu temelji za donošenje zakona (kroz međunarodne ugovore ili kroz nacionalne norme) čini ga moćnijim od većine nevladinih organizacija. U praksi, ISO se ponaša kao konzorcij usko povezan s vladama. Trenutno, ISO organizacija ima 165 članova od kojih svaki predstavlja svoju zemlju.[37]

U svojoj strategiji za razdoblje 2016-2020[38] (ISO, 2020) organizacija je za cilj postavila stvoriti globalno relevantne međunarodne standarde koji se koriste svugdje. U razdoblju od 2016. do 2020. godine krajnji se cilj, „ISO standardi koji se koriste svugdje“, ostvaruje kroz sljedeće strateške smjernice:

- **Razvoj standarda visoke kvalitete kroz globalno ISO članstvo** – Decentralizirana struktura ISO organizacije omogućava zemljama članicama prepoznavanje potreba pojedinog društva i lokalnog tržišta, angažiranje širokog spektra dionika, širenje standarda i podršku u njihovoj implementaciji.
- **Uključivanje dionika i partnera** – Učinkovit i dalekosežan angažman dionika koji je ključan u održavanju kredibiliteta ISO organizacije i važnosti Međunarodnih Standarda.
- **Razvoj ljudi i organizacija** – ISO investira u jačanje kapaciteta svih svojih članova, pojedinaca i organizacija, kroz učenje, istraživanje i razvoj.
- **Korištenje tehnologije** – Promjene u tehnologiji, izmjene u demografskoj strukturi stanovništva, promjene u društvenom ponašanju, prakticiranje kolaboracijskog načina

[37] International Organization for Standardization (2020). *About us*. Dostupno na: https://www.iso.org/about-us.html, pristupljeno 04.09.2020.
[38] International Organization for Standardization (2016). *ISO Strategy 2016-2020*. Dostupno na: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100364.pdf, pristupljeno 04.09.2020.

rada su novi izazovi za sva globalna poduzeća koja rade s informacijama, pa tako i za ISO.

- **Komunikacija** – Nacionalni ISO članovi nositelji su komunikacije vrijednosti i utjecaja ISO standarda prema svim zainteresiranima: donositeljima odluka u privatnom i u javnom sektoru, svim dionicima i općoj javnosti.

3.1. ISO istraživanje najzastupljenijih certifikata sustava upravljanja

Pregled certifikata je godišnje istraživanje broja važećih certifikata dobivenih prema ISO sustavima upravljanja koje se provodi diljem svijeta, a pružatelji podataka su akreditirana certifikacijska tijela.

U istraživanju iz 2018. godine[39] ukupni broj valjanih potvrda odnosno certifikata bio je manji nego u 2017. godini. Razlozi smanjenja mogu se razvrstati u tri kategorije: izostanak sudjelovanja nekih od certifikacijskih tijela, godišnje fluktuacije u podatcima nekih od certifikacijskih tijela te promjene u metodologiji prikupljanja podataka (je li uključen broj potvrda ili broj mjesta, promjene u nomenklaturi industrijskih sektora). Obrazloženja su sabrana prema sljedećem:

- Neka velika certifikacijska tijela prijavila su u prošlim istraživanjima broj potvrda koje su uključivale broj mjesta. U ovom su istraživanju podijelili broj potvrda i broj web mjesta što je dovelo do značajnog smanjenja broja prijavljenih certifikata.
- Podatci izviješteni od strane nekih velikih certifikacijskih tijela fluktuiraju iz godine u godinu.
- Neki davatelji podataka prilagodili su način prijavljivanja broja sektora obuhvaćenih njihovim certifikatima odvajanjem dvaju pitanja u anketnom upitniku za 2018. godinu,

[39] International Organization for Standardization (2019*). The ISO Survey of Management System Standard Certifications 2018*. Dostupno na: https://isotc.iso.org/livelink/livelink?func=ll&objId=20719433&objAction=browse&viewType=1, pristupljeno 04.03.2020.

a kako su u prošlim istraživanjima bili su povezani, to je dovelo do određenih nejasnoća u slučaju potvrda iz više sektora.

- Neka certifikacijska tijela koja su važna u nekim zemljama nisu sudjelovala.

U izvještaju su prikazane varijacije u broju certifikata od 2017. do 2018. godine. Uključeni su podatci onih pružatelja usluga koji su sudjelovali u istraživanju i 2017. i 2018. godine. Kako bi se osigurala valjana usporedba, nisu uključeni podatci davatelja usluga koji su sudjelovali samo u 1 od 2 istraživanja. U tablici nisu prikazani svi standardi obuhvaćeni istraživanjem zbog ograničene razine pouzdanosti/relevantnosti razlika i postotnih razlika između godišnjih podataka.

Tablica 10: Ukupan broj certifikata u tvrtkama koje su sudjelovale u istraživanju u obje godine, 2017. i 2018.

	Ukupan broj certifikata u tvrtkama koje su sudjelovale u istraživanju u obje godine, 2017. i 2018.			
Certifikati	**2017**	**2018**	**Razlika**	**Delta (%)**
ISO 9001:2015	758.344	739.206	-19.138	-3
ISO 14001:2015	251.343	258.566	7.223	3
ISO IEC 27001:2013	15.848	16.523	675	4
ISO 22000:2005&2018	26.652	27.091	439	2
ISO 13485:2003&2016	15.840	14.618	-1.222	-8
ISO 50001:2011	13.827	14.549	722	5

Izvor: ISO (2020), obrada autora

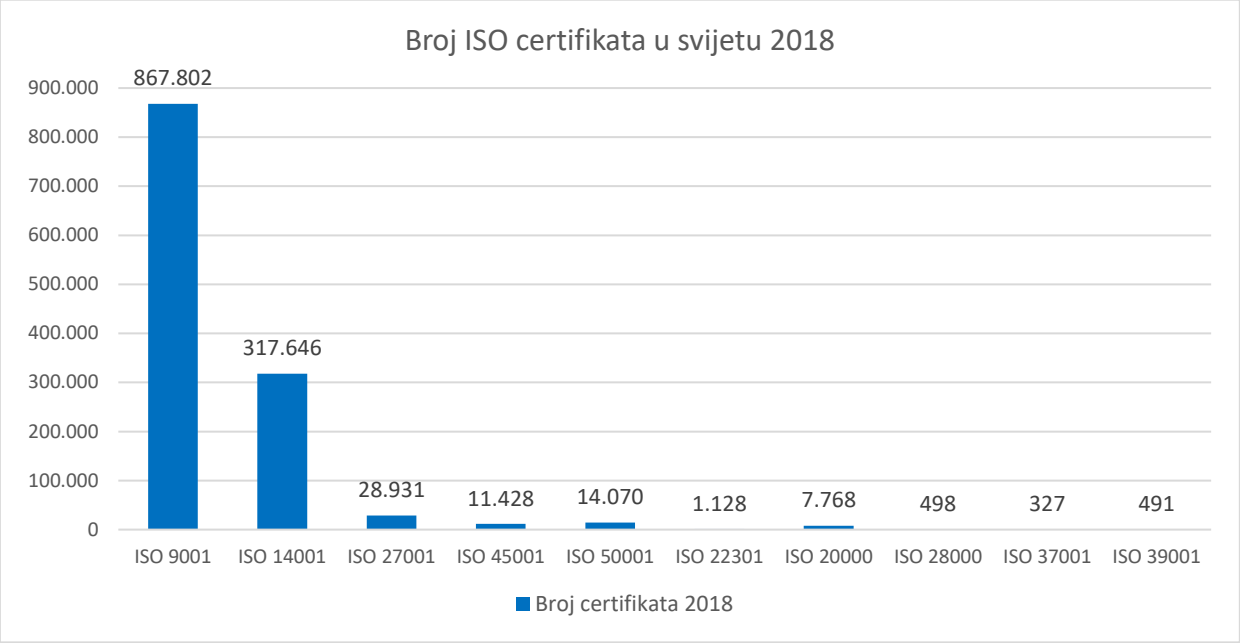
Iz usporedbe podatka vidljiv je pad broja ISO 9001 te osobito ISO 13485 certifikata. U slučaju ISO 9001 broj certifikata smanjen je za 3 % ili gotovo 2 tisuća, dok je kod ISO 13485 certifikata zabilježen pad od 8 % ili u apsolutnom iznosu 14.618 certifikata.

Postotno je u 2018. u odnosu na 2019. najviše narastao broj ISO 50001 - Upravljanje energijom, za 5%. Godišnji rast u broju certifikata zabilježen je i kod ISO IEC 27001 - Upravljanje sigurnosti informacija za 4%, i to s 15.848 certifikata u 2017. na 16.523 certifikata u 2018. godini.

Uz izdvojene ISO 14001 i ISO/IEC 27001 certifikate, u 2018. godini povećan je i broj ISO 14001 certifikata za 3 % i ISO 22000 certifikata za 2 %.

U istraživanju iz 2018. godine u svijetu je zabilježeno ukupno 1.250.089 različitih ISO certifikata. Najviše je ISO 9001 certifikata, 867.802 , odnosno 69,2 % od ukupnog broja. Pet najrasprostranjenijih, ISO 9001 – Sustavi upravljanja kvalitetom, ISO 14001 – Sustavi upravljanja okolišem, ISO/IEC 27001 – Sustavi upravljanja sigurnosti informacija, ISO 50001 – Sustavi upravljanja energijom i ISO 45001 – Sustav upravljanja zaštitom zdravlja i sigurnosti na radu, nose čak 99,2 % od ukupnog broja certifikata.

Grafikon 1: Broj ISO certifikata u svijetu 2018.

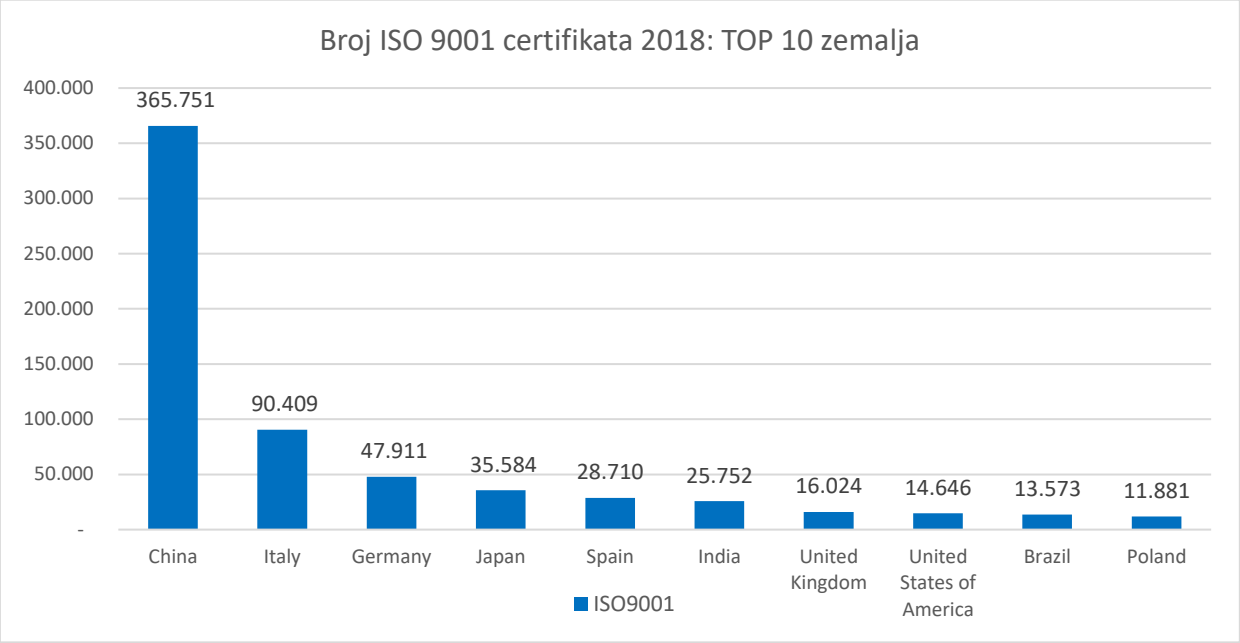


Izvor: ISO (2020), obrada autora

Očekivano, razlike između zemalja su značajne, tako da je Kina redovito na prvom mjestu, neovisno o kojem se certifikatu radilo. Također, u svim je zemljama zamjetna dominacija najstarijeg i najpoznatijeg ISO 9001 standarda.

Posjedovanje ISO 9001 standarda, uz Kinu na prvom mjestu, karakteristično je za europske zemlje. Tako se na ljestvici deset zemalja s najviše ISO 9001 certifikata u 2018. godini našlo pet europskih zemalja: Italija, Njemačka, Španjolska, Ujedinjeno kraljevstvo i Poljska. Od azijskih zemalja među prvih deset su Kina, Japan i Indija, dok američki kontinent predstavljaju dvije zemlje, SAD i Brazil.

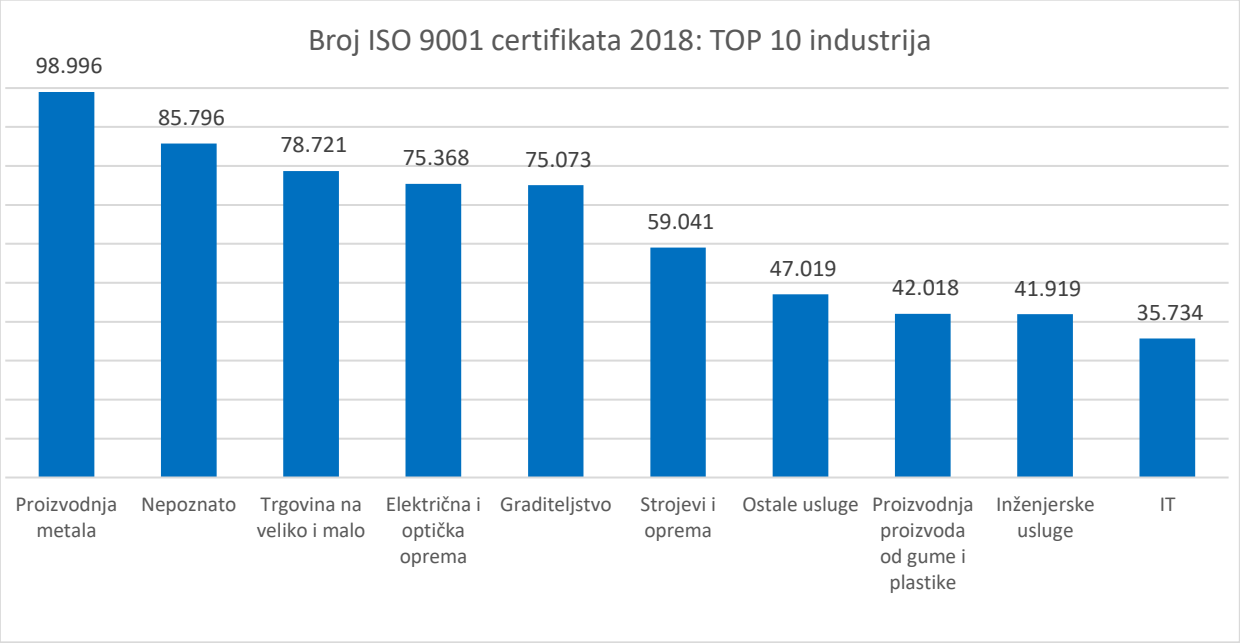
Grafikon 2: Broj ISO 9001 certifikata 2018.: TOP 10 zemalja



Izvor: ISO (2020), obrada autora

U izvještaju koji je objavila ISO organizacija, zanimljivi su i podatci o posjedovanju ISO 9001 standarda po industrijama. Na vrhu ljestvice nalaze metaloprerađivačka industrija, zatim veliki broj tvrtki nepoznate djelatnosti, a nakon njih djelatnosti trgovine, električne opreme i graditeljstva.

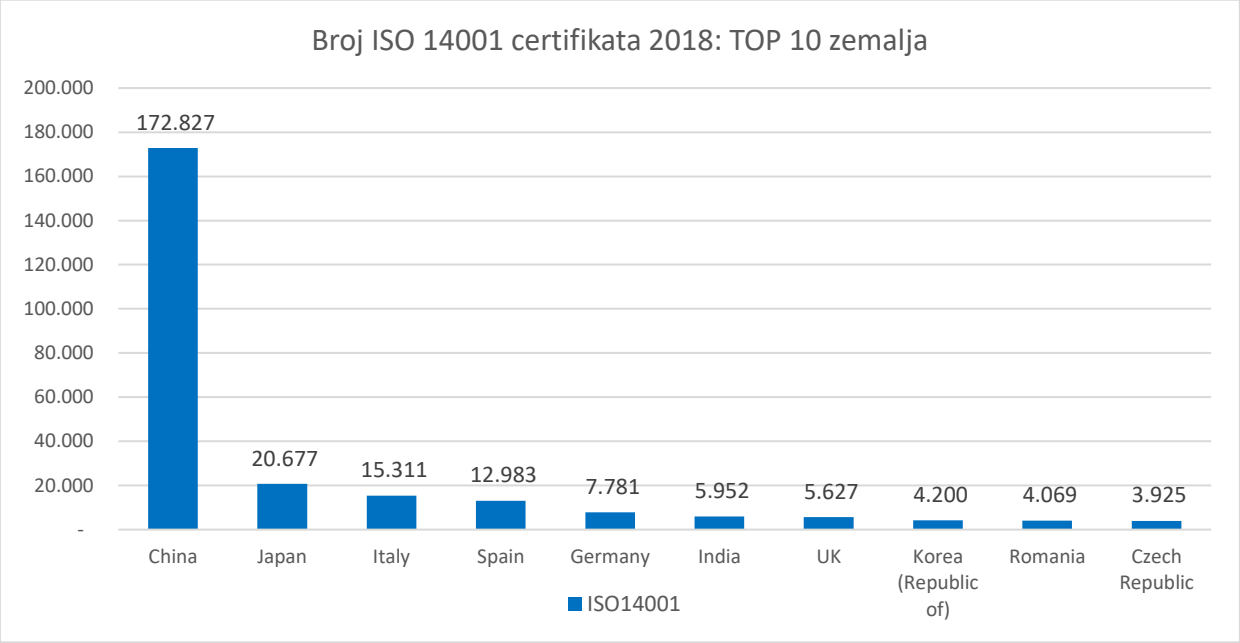
Grafikon 3: Broj ISO 9001 certifikata 2018.: TOP 10 industrija



Izvor: ISO (2020), obrada autora

Sljedeća ISO norma prema broju certifikata je ISO 14001 - Sustavi upravljanja okolišem. I u ovom slučaju na prvom mjestu je Kina s više od 170.000 certifikata u 2018. godini, a slijedi je Japan s 8,4 puta manjim brojem ISO 14001 certifikata. Od azijskih zemalja na ljestvici su se također našle Indija s 5.952 certifikata i Južna Korea s 4.200 certifikata. Preostalih šest vodećih zemalja su europske zemlje na čelu s Italijom.

Grafikon 4: Broj ISO 14001 certifikata 2018.: TOP 10 zemalja

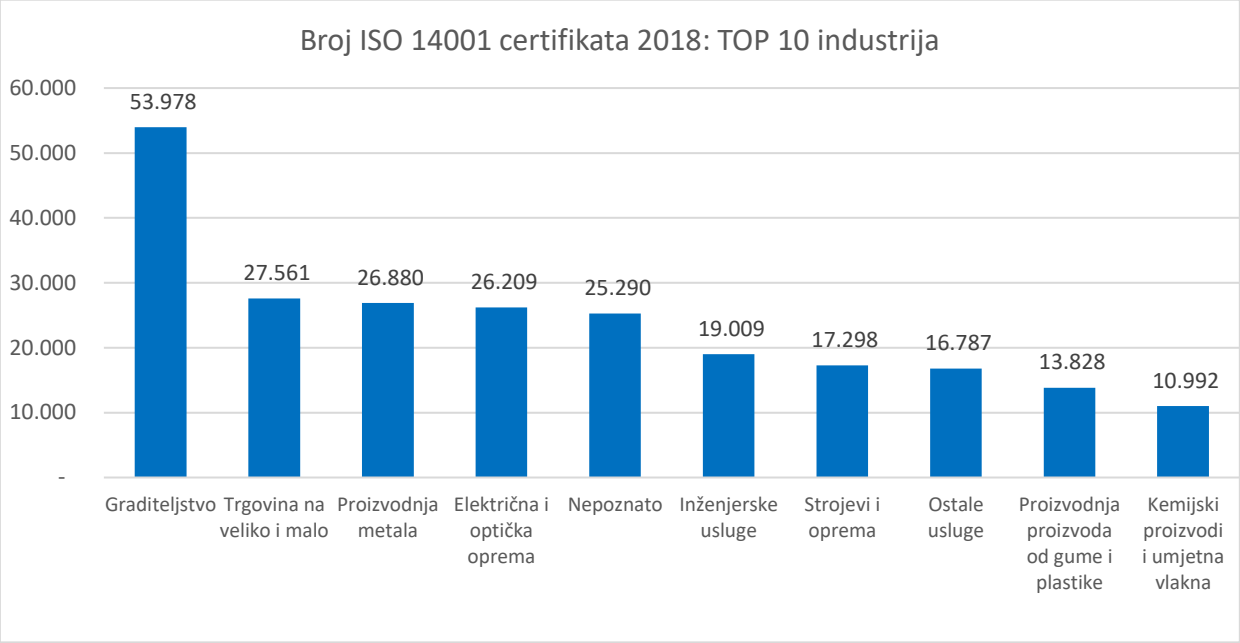


Izvor: ISO (2020), obrada autora

Posjedovanje ISO 14001 - Sustavi upravljanja okolišem najviše je zastupljeno u građevinskoj industriji na koju otpada 17%, odnosno 51.978 certifikata.

Sljedeća kategorija s nešto više od 25.000 certifikata su sektori trgovine, proizvodnje metala i električne opreme. Iako je ova međunarodna norma primjenjiva na svaku organizaciju bez obzira na njezinu djelatnost jer se odnosi na aktivnosti, proizvode i usluge koji su povezani s okolišem, među prvih 10 industrija dominiraju prerađivačke i proizvodne aktivnosti.

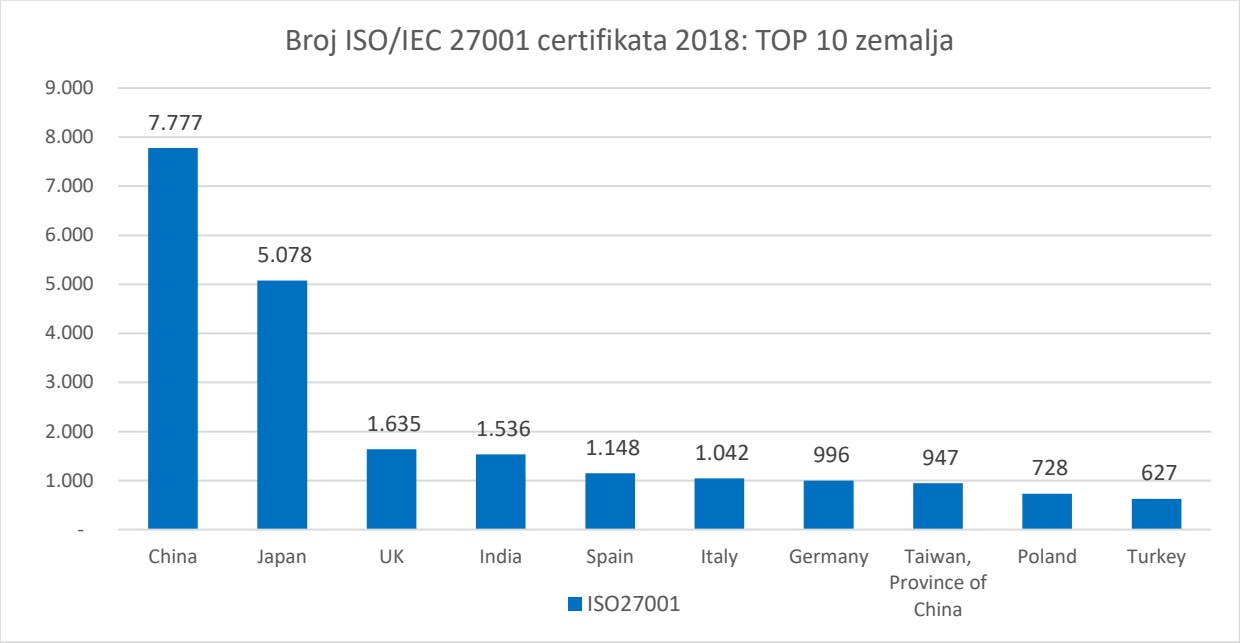
Grafikon 5: Broj ISO 14001 certifikata 2018.: TOP 10 industrija



Izvor: ISO (2020), obrada autora

ISO/IEC 27001 – Informacijska sigurnost je sljedeća norma u nizu prema broju certifikata. Iako je i kod ove norme prvo mjesto po broju certifikata zauzela Kina, prednost u odnosu na ostale zemlje nije izražena kao kod prethodna dva certifikata. Nakon Japana koji je na drugom mjestu s nešto više od pet tisuća certifikata, slijede uglavnom europske zemlje od kojih njih tri, Velika Britanija, Španjolska i Italija raspolažu s više od tisuću ISO/IEC 27001 certifikata.

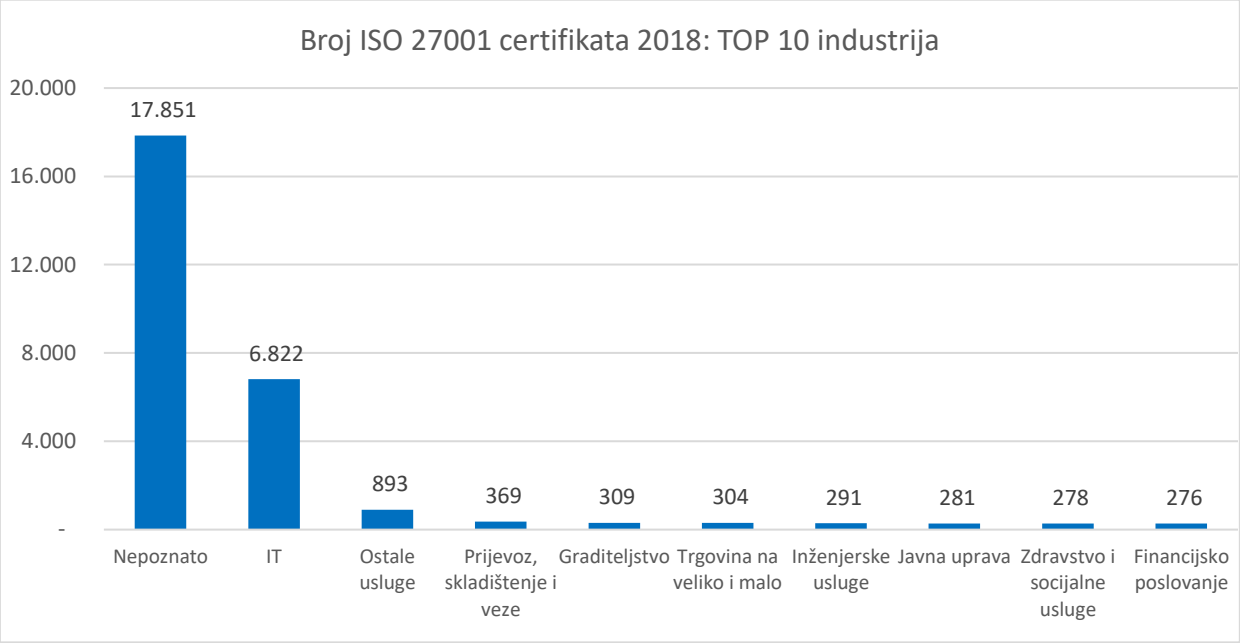
Grafikon 6: Broj ISO/IEC 27001 certifikata 2018.: TOP 10 zemalja



Izvor: ISO (2020), obrada autora

ISO/IEC 27001 nisu tehničke norme, nego norme upravljanja koje sadrže strukturirani set smjernica i specifikacija za pomoć organizacijama u razvoju sustava upravljanja informacijskom sigurnosti (ISMS – *Information Security Management System*). Stoga je zanimljivo pogledati koje industrije u većoj mjeri prepoznaju benefite uvođenja sustava informacijske sigurnosti. Prema podatcima iz ISO istraživanja 2018. godine, problematika informacijske sigurnosti najozbiljnije je shvaćena u industriji informacijske tehnologije. Sektor ostalih usluga, koji slijedi IT, ima gotovo osam puta manje ISO/IEC 27001 certifikata, a nakon njega slijede sektori prijevoza, graditeljstva i trgovine s 300 do 400 certificiranih za informacijsku sigurnost.

Grafikon 7: Broj ISO/IEC 27001 certifikata 2018.: TOP 10 industrija



Izvor: ISO (2020), obrada autora

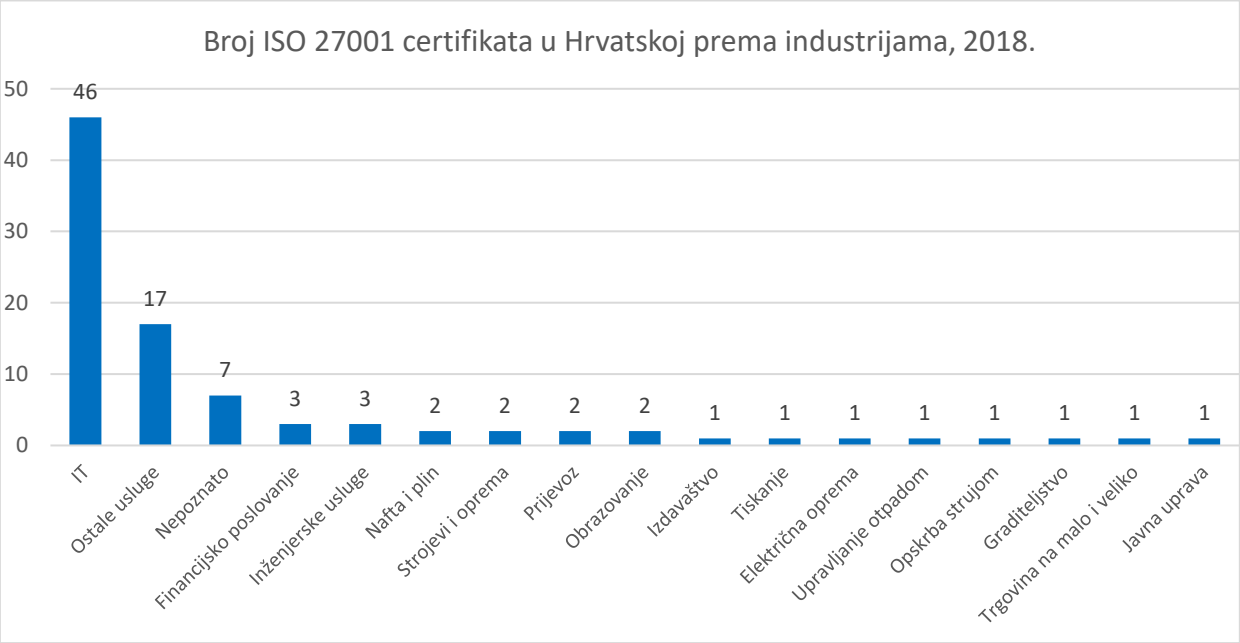
ISO/IEC 27001 u Hrvatskoj

Odjel za informacijsku sigurnost Zavoda za ispitivanje kvalitete 2005. je godine objavio distribucije lokaliziranih međunarodnih normi ISO/IEC 27001 i ISO 17799. Tada su nove verzije ovih najraširenijih normi za informacijsku sigurnost prvi put prevedene na hrvatski jezik kako bi se omogućila njihova primjena u zaštiti od gubitka, oštećenja i zloporabe povjerljivih informacija. Bankarski je sektor u RH je među prvima prepoznao problem s informacijskom sigurnošću i rano usvojio potrebu podizanja razine informacijske sigurnosti i zaštite osobnih podataka. Prema pisanju Poslovnog dnevnika, krajem 2005. godine u Hrvatskoj su bile certificirane dvije tvrtke.[40]

[40] Sesvečan. V. (2005). *Certifikat za ISO 27001 u Hrvatskoj imaju samo dvije tvrtke*, Poslovni dnevnik. Dostupno na https://www.poslovni.hr/sci-tech/certifikat-za-iso-27001-u-hrvatskoj-imaju-samo-dvije-tvrtke-372, pristupljeno 14.7.2020.

Prema ISO istraživanju broja certifikacija iz 2018. godine, Hrvatska je od tada napredovala te je u 2018. godini u hrvatskim organizacijama zabilježeno 138 ISO/IEC 27001 certifikata. Većina je certifikata u IT industriji, gotovo četvrtina, dok je na drugom mjestu sektor ostalih usluga sa 17 certifikata. U ostalim industrijama, broj certifikata je jednoznamenkast.

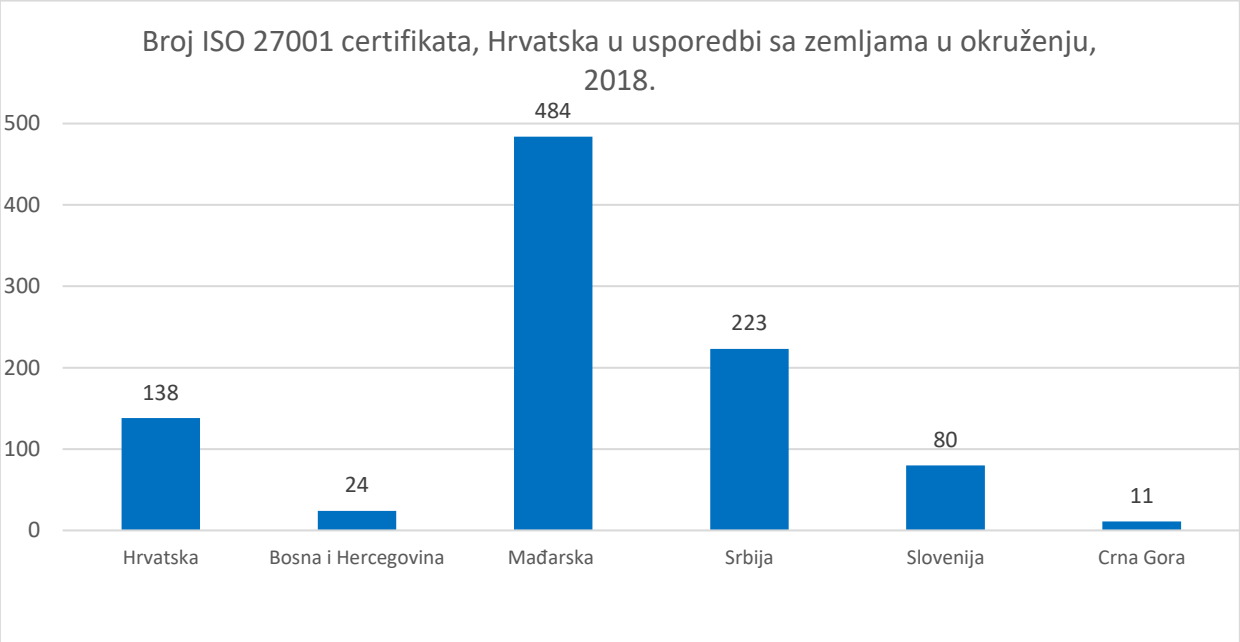
Grafikon 8: Broj ISO 27001 certifikata u Hrvatskoj prema industrijama, 2018.



Izvor: ISO (2020), obrada autora

U usporedbi sa zemljama s kojima graniči, Hrvatska je prema broju ISO/IEC 27001 certifikata na trećem mjestu, nakon Mađarske i Srbije. S obzirom na broj stanovnika u odnosu na navedene dvije zemlje koje su veće od Hrvatske, to nije loša pozicija. Očekivano, Hrvatska je ispred Bosne i Hercegovine i Crne Gore, ali i Slovenije.

Grafikon 9: Broj ISO 27001 certifikata, Hrvatska u usporedbi sa zemljama u okruženju, 2018.



Izvor: ISO (2020), obrada autora

3.2. Europske smjernice o standardizaciji i normizaciji

Opredijeljenost Europske unije prema standardizaciji, odnosno normizaciji vidljiva je i iz sadržaja Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća, recital 3.: „Europska normizacija također pomaže da se poveća konkurentnost poduzeća, posebno omogućavanjem slobodnog kretanja roba i usluga, interoperabilnosti mreža, komunikacijskih sredstava, tehnološkog razvoja i inovacija. Europska normizacija jača globalnu konkurentnost europske industrije, posebno kad je određena u koordinaciji s međunarodnim tijelima za normizaciju, točnije Međunarodnom organizacijom za normizaciju (ISO), Međunarodnom komisijom za

elektrotehniku (IEC) i Međunarodnom telekomunikacijskom unijom (ITU). Norme proizvode značajne pozitivne gospodarske učinke, na primjer promicanjem gospodarskog međusobnog prožimanja na unutarnjem tržištu te razvojem novih i poboljšanih proizvoda ili tržišta i poboljšanih uvjeta nabave. Norme tako obično povećavaju tržišno natjecanje i smanjuju troškove proizvodnje i prodaje, čime koriste gospodarstvu u cjelini, a posebno potrošačima. Norme mogu održavati i povećati kvalitetu, pružiti informacije i osigurati interoperabilnost i usklađenost, čime se povećava sigurnost i vrijednost za potrošače."[41]

Europska komisija u svom najnovijem dokumentu iz svibnja 2020. godine pod nazivom Tekući plan za IKT standardizaciju[42] ukazuje na snažnu opredijeljenost Europske unije ka sve opsežnijoj regulaciji i standardizaciji usluga i proizvoda vezanih uz IKT sektor te prvi put službeno ukazuje na konvergentnost ISO standarda u svojstvu zaštite sustava i podataka, osobito osobnih podataka. Tako su u dokumentu izrijekom prvi put u kombiniranom aspektu navedeni i ISO standardi vezani uz zaštitu privatnosti odnosno ISO/IEC 29100 – okvir za uspostavljanje zaštite privatnosti, ISO/IEC 27701 – sustav upravljanja informacijama o privatnosti iz 2019. godine koji predstavlja ekstenziju postojećeg ISO/IEC 27001 – sustava upravljanja informacijskom sigurnošću. U prosincu 2020. godine, Vijeće Europe, Europska komisija za učinkovitost pravosuđa (CEPEJ) u svojoj studiji izvodljivosti, objavljenoj u prosincu 2020. godine[43], prvi je put službeno klasificirala standard ISO/IEC 27701 kao standard koji „odražava najnovije dostignuće u pogledu zaštite privatnosti i, između ostalog, pokriva zahtjeve za stvaranje, implementaciju i poboljšanje sustava upravljanja informacijama o privatnosti (PIMS) i sigurnosna pitanja."

[41]Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća Tekst značajan za EGP, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?qid=1414068508676&uri=CELEX:32012R1025#ntr3-L_2012316HR.01001201-E0003, pristupljeno 23.11.2020.

[42] Europska komisija (2020). *Rolling plan for ICT standardisation 2020*. Dostupno na https://ec.europa.eu/docsroom/documents/41541, pristupljeno 28.12.2020.

[43] Vijeće Europe, Europska komisija za učinkovitost pravosuđa (CEPEJ) (2020). European Possible introduction of a mechanism for certifying artificial intelligence tools and services in the sphere of justice and the judiciary: Feasibility Study. Dostupno na: https://rm.coe.int/feasability-study-en-cepej-2020-15/1680a0adf4 , pristupljeno 16.12.2020.

3.2.1. ISO/IEC 29100:2011 i amandman ISO/IEC 29100:2011/AMD:2018 – Okvir za uspostavljanje zaštite privatnosti

„ISO/IEC 29100:2011 je međunarodni standard objavljen 2011. godine koji pruža okvir za uspostavljanje zaštite privatnosti koji definira zajedničku terminologiju, definira sve dionike i njihove uloge u obradi osobno identificirajućih podataka, opisuje razmatranja zaštite privatnosti te daje reference na poznata načela privatnosti u aspektima informacijskih tehnologija.[44]“

U svrhu razumijevanja konteksta privatnosti, u njemu su definirane osnovne terminološke karakteristike vezane uz razvoj daljnjih standarda koji se svojim strukturama dotiču tema privatnosti odnosno osobno identificirajućih podataka. Tijekom 2018. godine taj je standard dobio amandman (ISO/IEC 29100:2011/AMD:2018[45]) u kojem su djelomično revidirani pojedini pojmovi, a te revizije pojmova relevantne i su i u svim ostalim standardima gdje se izrijekom spominju.

„Okvir privatnosti u ovom međunarodnom standardu može poslužiti kao osnova za dodatne inicijative vezane uz standardizaciju privatnosti poput tehničke referentne arhitekture, primjene i uporabe specifičnih tehnologija privatnosti te cjelokupnog upravljanja privatnosti, kontrole privatnosti vezane uz vanjske procese nad podatcima, procjene rizika privatnosti i specifične tehničke specifikacije.[46]“

3.2.2. ISO/IEC 27001:2013 – Sustavi upravljanja informacijskom sigurnošću

„ISO/IEC 27001:2013 utvrđuje zahtjeve za uspostavljanje, primjenu, održavanje i kontinuirano poboljšanje sustava upravljanja informacijskom sigurnošću u kontekstu same organizacije te evidentira zahtjeve za procjenu i postupanje s rizicima informacijske sigurnosti prilagođene

[44] International Organization for Standardization (ISO), Dostupno na: https://www.iso.org/standard/45123.html, pristupljeno 30.11.2020.
[45] International Organization for Standardization (ISO), Dostupno na: https://www.iso.org/standard/73722.html, pristupljeno 30.11.2020.
[46] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2011). *Information Technology — Security Techniques — Privacy Framework* (ISO/IEC 29100:2011)

njenim potrebama. Zahtjevi utvrđeni u ISO/IEC 27001:2013 generički su i namijenjeni primjeni u svim organizacijama, bez obzira na vrstu, veličinu ili prirodu.[47]“

Sustav upravljanja informacijskom sigurnošću sadržan u ovom standardu namijenjen je očuvanju povjerljivosti, cjelovitosti i raspoloživosti informacija putem primjene kvalitativnog procesa upravljanja rizicima. Sam standard primjenjuje visokorazinsku strukturu te se temelji na tzv. Aneksu SL[48] ISO/IEC Direktive, Dio 1, Konsolidiranog ISO Dodatka, čime održava kompatibilnost s ostalim normama za sustave upravljanja koje su usvojile Aneks SL u smislu istovjetnosti terminologije.

Ured Vijeća za nacionalnu sigurnost je u izjavi o povezanosti usklađenosti informacijskog sustava sukladno standardu HRN ISO/IEC 27001/27002 i hrvatskim propisima informacijske sigurnosti naveo da su „u navedenoj normi određeni ciljevi koje organizacija treba postići kako bi imala učinkovit sustav zaštite svojih podataka te da se ISO 27002 bavi načinima, postupcima i najboljim praksama pomoću kojih se ti ciljevi mogu postići. U tom smislu je i tvrtka certificirana za HRN ISO/IEC 27001 usklađena i s hrvatskim propisima informacijske sigurnosti koji vrijede isključivo za neklasificirane podatke (NN 46/08, Uredba o mjerama informacijske sigurnosti, čl. 8.). Uspješna provedba norme kao što je ISO/IEC 27001, može olakšati provedbu propisanih mjera i standarda informacijske sigurnosti jer su neki sigurnosni zahtjevi slični te sama realizacija može biti lakše usklađena“.[49]

3.2.3. ISO/IEC 27002:2013 – Kodeks postupanja s kontrolama informacijske sigurnosti

ISO/IEC 27002:2013 je standard koji daje smjernice vezane uz praksu postupanja u ispunjavanjima zahtjeva kontrola informacijske sigurnosti definiranima u ISO/IEC 27001:2013

[47] International Organization for Standardization (ISO), Dostupno na: https://www.iso.org/standard/54534.html, pristupljeno 01.12.2020.
[48] International Organization for Standardization (ISO*), ISO/IEC Directives, Part 1, Consolidated ISO Supplement, - Procedures specific to ISO*, Dostupno na: https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor535, pristupljeno 5.1.2021.
[49] Republika Hrvatska, Ured vijeća za nacionalnu sigurnost (2020). *Informacijska sigurnost – NSA*, Dostupno na: https://www.uvns.hr/hr/ako-je-informacijski-sustav-uskladjen-s-hrn-iso-iec-27001-27002-je-li-uskladjen-i-s-hrvatskim-propisima-informacijske-sigurnosti-o-informacijskim-sustavima, pristupljeno 29.9.2020.

te uključuje odabir, provedbu i upravljanje kontrolama s obzirom na okruženje same organizacije[50]

3.2.4. ISO/IEC 27701:2019 – Sustavi upravljanja informacijama o privatnosti

„ISO/IEC 27701:2019 je standard izdan 2019. godine koji specificira konkretne zahtjeve i pruža smjernice za uspostavljanje, primjenu i kontinuirano poboljšavanje sustava za upravljanje informacijama o privatnosti (*Privacy Information Management System – PIMS*). Primjenjiv je na sve vrste i veličine organizacija, uključujući javne i privatne subjekte, vladine i neprofitne organizacije, koje su voditelji ili izvršitelji obrada osobnih podataka obrađivanih unutar sustava upravljanja informacijskom sigurnošću u organizaciji[51]“

Standard sadrži zahtjeve i smjernice za voditelje i izvršitelje obrade koji su odgovorni za pouzdanost obrade osobnih podataka unutar sustava upravljanja informacijskom sigurnošću. Standard predstavlja dopunu normi ISO/IEC 27001 i ISO/IEC 27002 u aspektima sigurnosnih tehnika za upravljanje informacijama o privatnosti te se aplicira u kombinaciji s njima. Standard je potrebno interpretirati uzimajući u obzir lokalnu legislativu i/ili regulativu.

[50] International Organization for Standardization (ISO), Dostupno na: https://www.iso.org/standard/54533.html, pristupljeno 27.12.2020.
[51] International Organization for Standardization (ISO), Dostupno na: https://www.iso.org/standard/71670.html, pristupljeno 27.12.2020.

4. Model procjene sustava upravljanja informacijskom sigurnošću i privatnošću u analizi stanja i reviziji usklađenosti organizacijskih i tehničkih mjera postojećeg sustava s ISO/IEC 27001 i ISO/IEC 27701 i/ili Uredbom i nacionalnim provedbenim zakonom

NPISPMSA[52] model sustava upravljanja informacijskom sigurnošću i privatnošću temelji se na metodologiji *benchmarkinga*[53] te predstavlja kombiniran sustav (ISMS[54] i PIMS[55]) mapiranih audit pitanja vezanih uz Uredbu s izdvojenim kontrolama, zahtjevima, dopunom stavaka iz nacionalnog provedbenog zakona te taksonomijom i smjernicama za auditiranje iz pet ISO i ISO/IEC standarda. To podrazumijeva i zahtjeve kontrola iz Aneksa A ISO/IEC 27001, kodeksa postupanja s kontrolama informacijske sigurnosti definiranih u ISO/IEC 27002 te ekstenzije ISO/IEC 27701 s Aneksima A za voditelje obrade i Aneksa B za izvršitelje obrade, taksonomije privatnosti ustanovljene u ISO/IEC 29100 integrirane s tehnikama auditiranja propisanih smjernicama za auditiranje sustava upravljanja u standardu ISO 19011.

Model sadrži ukupno 272 mapirana audit pitanja s klasifikacijama sukladnosti, nesukladnosti i izuzeća primjenjivosti uz obrazloženje izuzeća i evidencijom prilika za poboljšanje, te evidentiranjem audit dokaza, korektivnih radnji i zadanog roka rješavanja identificiranih nesukladnosti. Audit upitna lista sadrži 220 pitanja vezana uz regulatorne zahtjeve i zahtjeve kontrola iz normativnog Aneksa A ISO/IEC 27001, kodeksa postupanja s kontrolama definiranim u ISO/IEC 27002 i zahtjeva ISO/IEC 27701 te ukupno 52 pitanja izvedenih iz kontrola specifičnih aneksa odnosno 34 pitanja vezano uz normativni Aneks A za voditelje obrade i 18 pitanja vezanih uz normativni Aneks B za izvršitelje obrade.

Međunarodni ISO/IEC standardi pregled su najboljih globalnih praksi ustanovljen tehnikama kompetitivne analize zbog čega se veliki broj zakona i propisa oslanja upravo na njih. Ovaj

[52] *NPISPMSA – NP Information Security and Privacy Management System Assessment/Audit*
[53] *Benchmarking* – metoda kojom neka organizacija identificira i istražuje ključne aspekte nekog drugog entiteta (koji na temelju određenih kriterija zaslužuje biti mjera vrijednosti), a saznanja dobivena njime primjenjuje u unaprjeđivanju vlastitih procesa (Kopal i Korkut, 2014).
[54] ISMS (*Information Security Management System*) – Sustav upravljanja informacijskom sigurnošću, koristi se kao skraćenica za ISO/IEC 27001
[55] PIMS (*Privacy Management System*) – Sustav upravljanja informacijama o privatnošću, koristi se kao skraćenica za ISO/IEC 27701

model se može koristiti u analizi stanja usklađenosti organizacijskih i tehničkih mjera sa zahtjevima propisanim Općom uredbom o zaštiti podataka i/ili usklađenosti postojećeg sustava s predmetnim standardima u svrhu internog audita, audita druge strane ili certifikacijskog audita (audita treće strane).

Kao i predmetne ISO/IEC standarde, model mogu koristiti organizacije svih vrsta i veličina, javne i privatne, kao i državna tijela te neprofitne organizacije koje su voditelji obrade i/ili izvršitelji obrade osobnih podataka neovisno o tome imaju li već u svojoj organizaciji uspostavljen sustav upravljanja informacijskom sigurnošću ili posjeduju ISO/IEC 27001 certifikat. Model analize stanja i procjene učinkovitosti služi kao kvalitativan alat pri usklađivanju organizacijskih i tehničkih mjera organizacija s Uredbom i/ili kontrolama proširenog ISO/IEC 27001 sustava upravljanja informacijskom sigurnosti.

Kod organizacija koje nemaju implementirane ISO/IEC standarde, a žele uskladiti postojeće organizacijske i tehničke mjere s Uredbom i nacionalnim provedbenim zakonom ili uvesti sustav upravljanja informacijskom sigurnošću i privatnošću u menadžment organizacijskih procesa ustanovljen opsegom, model služi za analizu trenutnog stanja usklađenosti kontrola u sustavu informacijske sigurnosti i privatnosti te organizacijskih i tehničkih mjera. Svojom evidencijom klasifikacije dosegnute razine pojedinog zahtjeva i komentara predstavlja kvalitativan prikaz usklađenih područja i područja za poboljšanja identificiranih stavki.

Kod organizacija koje imaju implementirane ISO/IEC standarde ili posjeduju certificirane sustave, model predstavlja kvalitativan okvir za proširenje postojećeg sustava i/ili provedbu audita i izvještavanja o rezultatima istog, bilo da se radi o internom auditu, auditu druge ili pak auditu treće strane.

Model mogu koristiti sve razine auditora – interni, vodeći i certifikacijski auditori, uz nužnost prethodnog poznavanja sadržaja i primjene Uredbe, nacionalnog provedbenog zakona, kao i ostale nacionalne regulative vezane uz zaštitu osobnih podataka ili informacijsku sigurnost u pojedinoj zemlji korištenja modela.

4.1. Taksonomija standarda i „osobni podatak“

Na temelju prava EU-a, kao i na temelju prava Vijeća Europe, osobni su podatci definirani kao informacije koje se odnose na „identificiranu fizičku osobu ili fizičku osobu koju se može identificirati“[56]. To se odnosi na informacije o osobi čiji je identitet sasvim jasan ili ga je barem moguće utvrditi kombinacijom različitih prikupljenih podataka. „Kako bi se odredilo može li se identitet pojedinca utvrditi, voditelj obrade ili bilo koja druga osoba mora uzeti u obzir sva sredstva koja se, po svemu sudeći, mogu upotrijebiti u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca, poput primjerice selekcije, koja omogućuje da se s jednom osobom postupa drugačije od drugih“[57]. Ako se podatci o takvoj osobi obrađuju, ona se naziva „ispitanik”.

U usklađivanju organizacija s Uredbom i nacionalnim provedbenim zakonom primjenom međunarodnih standarda ISO/IEC 27001 i ekstenzije ISO/IEC 27701 preporučljivo je kombinirati najmanje pet ISO standarda:

1. ISO/IEC 27001 Sustavi upravljanja informacijskom sigurnošću
2. ISO/IEC 27002 Kodeks prakse kontrola informacijske sigurnosti
3. ISO/IEC 27701 Sustav upravljanja informacijama o privatnosti
4. ISO/IEC 29100 Okvir za zaštitu privatnosti
5. ISO 19011 Smjernice za auditiranje sustava upravljanja

Standard ISO/IEC 27701 definirao je lokacije zahtjeva i nadopuna specifičnih za PIMS u obje norme uz napomenu da se proširena interpretacija informacijske sigurnosti u njihovom sadržaju uvijek primjenjuje (čak i kada pojedini zahtjev ne sadrži zahtjeve specifične za PIMS) te terminološki glasi: ***informacijska sigurnost i privatnost***.

Za korištenje NPISPMSA modela sustava upravljanja informacijskom sigurnošću pomoću ISO/IEC 27001 i ekstenzije ISO/IEC 27701 u procjeni usklađenosti razine organizacijskih i

[56] Opća uredba o zaštiti podataka, članak 4. stavak 1.; modernizirana Konvencija br. 108, članak 2. točka (a).
[57] Opća uredba o zaštiti podataka, uvodna izjava 26.

tehničkih mjera, uz terminologiju vezanu uz informacijsku sigurnost neophodno je i poznavanje terminologije vezane uz privatnost i zaštitu osobnih podataka jer su predmetne norme bazirane na Aneksu SL koji omogućava, ali i uvjetuje njihovu konvergentnost.

U nastavku slijede preneseni pojmovi i njihove definicije.

ISO/IEC 29100:2011 i amandman ISO/IEC 29100:2011/AMD:2018 – Okvir za zaštitu privatnosti:

- **„2.9. Osobni identificirajući podatci (PII)[58]**
    - Svaki podatak koji (a) se može koristiti za uspostavljanje poveznice između podataka i fizičke osobe na koju se odnose takvi podatci, ili (b) svaki podatak koji je ili može biti izravno ili neizravno povezan s fizičkom osobom; uz napomenu da je „fizička osoba“ u definiciji principal PII-a (2.11). Kako bi se utvrdilo je li moguće utvrditi identitet principala PII-a, treba uzeti u obzir sva sredstva koja razumno mogu koristiti nositelji privatnosti koji čuvaju podatke, ili neka druga strana, kako bi se utvrdila veza između seta PII-a i fizičke osobe.“

- **„2.20 AMD 2018 Procjena utjecaja na privatnost (PIA)[59]**
    - Procjena rizika privatnosti - cjelokupni proces identificiranja, analize, procjene, konzultiranja, komunikacije i planiranja rješavanja potencijalnih utjecaja na privatnost vezano za obradu osobnih identificirajućih podataka, a kao dio šire slike upravljanja rizicima unutar organizacije.

- **„4.2.1 Principali osobno identificirajućih podataka (PII)[60]**
    - Principali PII-a pružaju svoje PII za obradu voditeljima i izvršiteljima obrade PII-a i, kada nije drugačije navedeno primjenjivim zakonom, oni daju odobrenje i utvrđuju svoje preferencije vezane za privatnost o tome kako bi njihove PII trebalo obraditi. Principali PII-a mogu uključivati npr. zaposlenika navedenog u sustavu

[58] Ibid.
[59] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2018). *Information Technology — Security Techniques — Privacy Framework — Amendment 1: Clarifications* (ISO/IEC 29100:2011/AMD 1:2018)
[60] Ibid.

odjela ljudskih resursa nekog društva, klijenta navedenog na kreditnom izvještaju i bolesnika navedenog u elektroničkoj zdravstvenoj evidenciji. Nije uvijek potrebno da određena fizička osoba bude izravno identificirana imenom kako bi se ona smatrala principalom PII-a. Ako se fizička osoba na koju se odnose PII može indirektno identificirati (npr. preko identifikatora računa, matičnog broja ili kroz kombinaciju dostupnih faktora), on ili ona smatra se principalom PII-a za taj set PII-a.„

- **„4.2.2 Voditelji obrade osobno identificirajućih podataka (PII)[61]**
    - Voditelj obrade PII-a utvrđuje zašto (svrhu) i kako (sredstvo) će se obrada PII dogoditi. Voditelj obrade treba osigurati pridržavanje principa privatnosti unutar ovog okvira tijekom obrade PII-a pod njegovom kontrolom (npr. implementirajući potrebne kontrole privatnosti). Može biti više od jednog voditelja obrade za isti set PII-a ili set operacija koje se izvršavaju na PII-ma (zbog iste ili različite legitimne svrhe). U tom slučaju različiti voditelji obrade će surađivati zajedno i napraviti određene mjere kako bi osigurali pridržavanje principa privatnosti tijekom obrade PII-a. Voditelj obrade također može odlučiti želi li da sve ili dio operacija obrade izvrše drugi nositelji privatnosti u njegovo ime. Svi voditelji obrade trebaju pažljivo procijeniti obrađuju li ili ne osjetljive PII-e i implementirati razumne i odgovarajuće kontrole za privatnost i sigurnost temeljene na zahtjevima navedenim u relevantnim nadležnostima, kao i sve potencijalne štetne učinke za principale PII-a kako je identificirano tijekom procjene rizika privatnosti.“

- **„4.2.3 Izvršitelj obrade osobno identificirajućih podataka (PII)[62]**
    - Izvršitelj obrade provodi obradu PII-a u ime voditelja obrade, djeluje u ime ili sukladno uputama voditelja obrade PII-a, pridržava se definiranih zahtjeva za privatnost i implementira odgovarajuće kontrole privatnosti. U nekim nadležnostima izvršitelj obrade vezan je pravnim sporazumom.“

[61] Ibid.
[62] Ibid.

- **„2.9 AMD 2018 Osobno identificirajući podatci (PII)[63]**
    - Svaki podatak koji (a) se može koristi za utvrđivanje identiteta principala PII-a na kojeg se takvi podatci odnose, ili (b) svaki podatak koji može izravno ili neizravno biti povezan s principalom; uz napomenu da kako bi se utvrdilo je li principalu moguće utvrditi identitet, treba uzeti u obzir sva sredstva koja razumno mogu upotrijebiti nositelji privatnosti koji čuvaju podatke, ili bilo koja druga strana, kako bi utvrdili identitet te fizičke osobe.“

- **„2.10 Voditelj obrade PII-a[64]**
    - Nositelj privatnosti (ili nositelji privatnosti) koji utvrđuje svrhe i sredstva za obradu osobno identificirajućih podataka (PII) a koji nije fizička osoba koja koristi podatke u osobne svrhe; uz napomenu da voditelj obrade PII-a nekada nalaže drugima (npr. izvršiteljima obrade) da obrade PII u njegovo ime dok odgovornost za obradu ostaje i dalje na njemu.“

- **„2.11 Principal osobno identificirajućih podataka (PII)[65]**
    - Fizička osoba na koju se odnose osobni identificirajući podatci (PII); uz napomenu da se ovisno o nadležnosti i primjenjivim zakonima za zaštitu privatnosti i podataka, sinonim „ispitanik“ (*data subject*) može također koristiti umjesto pojma principal PII-a.“

[63] Ibid.
[64] Ibid.
[65] Ibid.

ISO/IEC 27701:2019 – Sustavi upravljanja informacijama o privatnosti

- **„3.1 Zajednički voditelj obrade osobno identificirajućih podataka (PII)**
  - Voditelj obrade osobno identificirajućih podataka utvrđuje svrhu i sredstva obrade osobno identificirajućih podataka zajedno s jednim ili više drugih voditelja obrade osobno identificirajućih podataka.[66]“

- **„3.2 Sustav upravljanja informacijama o privatnosti (PIMS)**
  - Sustav upravljanja informacijskom sigurnošću koji se odnosi na zaštitu privatnosti kao potencijalno ugroženu obradom osobno identificirajućih podataka.[67]“

- Dodatni termin u standardu jest i „**klijent**“ koji je definiran točkom 4.4:
  - „Ovisno o ulozi organizacije, „klijent“ se može tumačiti kao: a) organizacija koja ima ugovor s voditeljem obrade (npr. klijent voditelja obrade), u slučaju kada je organizacija zajednički voditelj obrade, a pojedinac koji je u direktnom poslovnom odnosu s organizacijom (B2C) naziva se „principalom osobno identificirajućih podataka“ u ovom dokumentu, b) voditelj obrade koji ima ugovor s izvršiteljem obrade (npr. klijent izvršitelja obrade); ili c) izvršitelj obrade koji ima ugovor s podugovoriteljem za obradu PII-a (npr. klijent podugovorenog podizvršitelja obrade PII-a).[68]“

Pojam „osobno identificirajući podatak“ u modelu je iskazan istoznačnicom odnosno pojmom „osobni podatak“ ili „PII“ (*Personally Identifiable Information - PII*), dok je pojam „principal osobno identificirajućih podataka“ iskazan istoznačnicom odnosno pojmom „ispitanik“ i predstavlja osobu čiji se osobni podaci obrađuju.

[66] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2019). *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines* (ISO/IEC 27701:2019)

[67] Ibid.

[68] Ibid.

4.2. Analiza strukture ISO/IEC 27701 i ISO/IEC 27002 standarda u odnosu na strukturu ISO/IEC 27001 i analitički proces u prikupljanju i obradi podataka

ISO/IEC 27001 - Sustavi upravljanja informacijskom sigurnošću međunarodni je standard u kojem su detaljno navedeni zahtjevi za uspostavljanje, provedbu, održavanje i kontinuirano poboljšavanje sustava informacijske sigurnosti u službi povećanja sigurnosti informacijske imovine organizacije. Standard se sastoji od dva odvojena dijela, odnosno od klauzula sa zahtjevima i smjernica s ciljevima i kontrolama njihovog nadzora. Prvi dio sastoji se od 11 klauzula, a drugi dio predstavlja tzv. Aneks A (*Annex A*) u kojem je navedeno 114 ciljeva i kontrole nadzora. Standard se temelji na kvalitativnom upravljanju rizicima. Ispunjavanje zahtjeva ciljeva i kontrola navedenih u Aneksu A ISO/IEC 27001 standarda detaljno su u obliku smjernica definirani u standardu ISO/IEC 27002, koji predstavlja kodeks prakse kontrola informacijske sigurnosti u usklađivanju sa standardom ISO/IEC 27001.

Prvi dio standarda ISO/IEC 27001 je obavezan za sve organizacije u usklađivanju poslovanja i poslovnih praksi s njime, dok dio s Aneksom A ovisi o definiranom točnom opsegu uvođenja sustava upravljanja informacijskom sigurnošću i procesima unutar same organizacije; odnosno, pojedine je kontrole moguće isključiti ako organizacija ima pravovaljano, dokumentirano i odobreno obrazloženje za njihovo isključivanje. Uvjet isključenja pojedine kontrole svakako je da njezino isključenje ne utječe na stabilnost uspostave informacijske sigurnosti u cijeloj organizaciji odnosno definiranom opsegu (primjerice, nije moguće isključiti kontrole vezane uz upravljanje rizicima, dok je, ukoliko organizacija nema razvoj vlastitog softvera, moguće uz detaljno obrazloženje isključiti kontrolu vezanu uz siguran razvoj).

Standard ISO/IEC 27701, predstavljen tijekom kolovoza 2019. godine, dopuna je standarda ISO/IEC 27001 i ISO/IEC 27002 i daje zahtjeve i smjernice za upravljanje o informacijama o privatnosti koje se sadržajno obvezno dopunjuju na točno definirane zahtjeve i smjernice u prva dva standarda te postavlja i dodatne zahtjeve i smjernice vezane uz voditelje i izvršitelje obrade, koji su odgovorni za obradu osobnih podataka. Odnosi se na organizacije svih vrsta i veličina, uključujući javna i privatna trgovačka društva, državna tijela i neprofitne organizacije te se implementira u sklopu uvođenja informacijske sigurnosti u organizaciju.

Korelacijske tablice (Tablica 37. i 38.) s lokacijama specifičnih zahtjeva i drugih informacija za implementaciju kontrole u vezanim standardima predstavljaju smjernice za razumijevanje zahtjeva i smjernica i/ili mjesta potrebnih adaptacija u postojećim ISO/IEC sustavima organizacije.

Tablica 11. - Lokacija zahtjeva specifičnih za PIMS i drugih informacija za implementaciju kontrole u standardu ISO/IEC 27001:2013(E)

Članak u normi ISO/IEC 27001:2013(E)	Naslov	Podklauzula u ovom dokumentu	Primjedbe
4	Kontekst organizacije	5.2	Dodatni zahtjevi
5	Vođenje	5.3	Nema zahtjeva specifičnih za PIMS
6	Planiranje	5.4	Dodatni zahtjevi
7	Podrška	5.5	Nema zahtjeva specifičnih za PIMS
8	Provedba	5.6	Nema zahtjeva specifičnih za PIMS
9	Vrednovanje učinkovitosti	5.7	Nema zahtjeva specifičnih za PIMS
10	Poboljšanje	5.8	Nema zahtjeva specifičnih za PIMS

Izvor: ISO/IEC 27701:2019

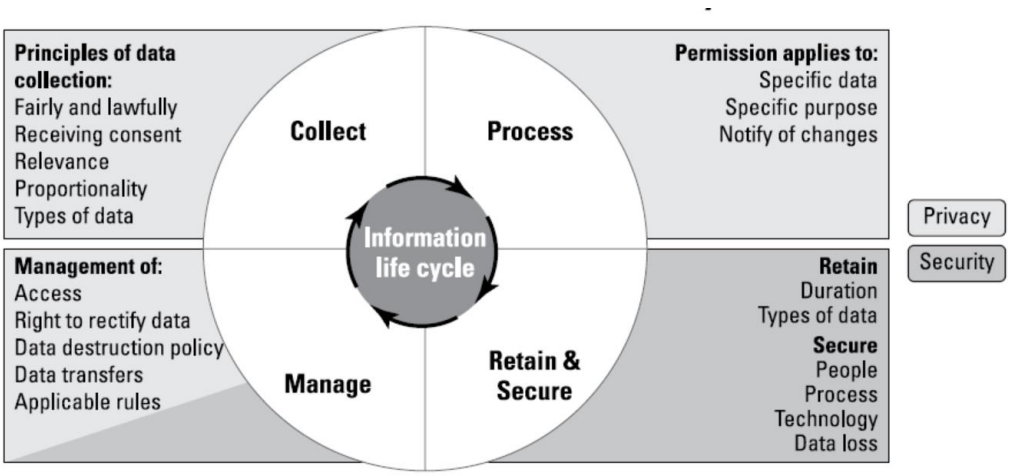
Tablica 12. - Lokacija zahtjeva specifičnih za PIMS i drugih informacija za implementiranje kontrola u standardu ISO/IEC 27002:2013(E)

Članak u normi ISO/IEC 27002:2013	Naslov	Podklauzula u ovom dokumentu	Primjedbe
5	Politike informacijske sigurnosti	6.2	Dodatne smjernice
6	Organizacija informacijske sigurnosti	6.3	Dodatne smjernice
7	Sigurnost ljudskih resursa	6.4	Dodatne smjernice
8	Upravljanje imovinom	6.5	Dodatne smjernice
9	Kontrola pristupa	6.6	Dodatne smjernice
10	Kriptografija	6.7	Dodatne smjernice
11	Fizička sigurnost i sigurnost povezana s okolišem	6.8	Dodatne smjernice
12	Sigurnost operacija	6.9	Dodatne smjernice
13	Sigurnost komunikacija	6.10	Dodatne smjernice
14	Nabava, razvoj i održavanje sustava	6.11	Dodatne smjernice
15	Odnosi s dobavljačima	6.12	Dodatne smjernice
16	Upravljanje slučajevima vezanim za informacijsku sigurnost	6.13	Dodatne smjernice
17	Aspekti informacijske sigurnosti za upravljanje kontinuitetom poslovanja	6.14	Nema zahtjeva specifičnih za PIMS
18	Sukladnost	6.15	Dodatne smjernice

Izvor: ISO/IEC 27701:2019

Proširenje sustava informacijske sigurnosti s aspektima vezanim uz ophođenje s informacijama o privatnosti odnosno osobnim podatcima podrazumijeva i razumijevanje cjelokupnog procesa koji se događa otkad pojedini osobni podatak počinje teći bilo kojim organizacijskim sustavom, odnosno ulazi u sferu nekog od njenih unutarnjih procesa (uključujući i odnose s vanjskim dionicima). Pojmovi vezani uz obradu osobnih podataka uključuju njihovo prikupljanje, obradu i arhiviranje, a pravilno postupanje zahtijeva i uvođenje određenih organizacijskih i tehničkih mjera u svojstvu njihove zaštite. Na Slici 18. prikazan je životni ciklus pojedine informacije odnosno osobnog podatka i zahtjeva vezanih uz njegovo pravno utemeljeno ophođenje.

Slika 18: Životni ciklus informacije prema Općoj uredbi o zaštiti podataka



Izvor: *The GDPR & Managing Data Risk* Symantec Special Edition (2018:10)

Proces prikupljanja podataka o administriranju i pravnoj utemeljenosti obrada nad osobnim podatcima trebao bi biti temeljen na *intelligence* procesu koji se sastoji od šest koraka (Kopal i Korkut, 2020:23): „(1) Faza planiranja odnosno utvrđivanje potreba tvrtke ili organizacije, zahtjeva i izrade plana prikupljanja podataka odnosno smjernica pojedinih aktivnosti vezanih uz samo prikupljanje podataka; (2) faza prikupljanja podataka koja se provodi usmjereno i fokusirano iz svih dostupnih izvora unutar ili izvan organizacije; (3) procjena ili klasifikacija podataka odnosno razvoj zaključaka s obzirom na točnost i pouzdanost podataka; (4) obrada ili organiziranje podataka koje se odnosi na pohranu podataka i upućivanje na te podatke u svrhu njihovog kasnijeg pronalaženja (tzv. indeksirano unakrsno referenciranje); (5) analiza odnosno procjena, interpretacija i međusobno povezivanje u svrhu otkrivanja obrasca ili značenja induktivnom logikom i (6) razdioba odnosno prijenos gotovog analitičkog proizvoda krajnjim korisnicima.“

4.3. Analitički proces u donošenju zaključaka i smjernice za auditiranje vezane uz ISO 19011

Korištenje modela podrazumijeva proces prikupljanja podataka sukladno navedenoj *intelligence* metodologiji i donošenje zaključaka temeljenih na dokazima i argumentima prema sljedećim indikatorima vezanim uz učinkovitost sustava:

1. Sukladnost, odnosno usklađenost sa zahtjevom (*Conformity – C*)
2. Nesukladnost, odnosno neusklađenost (*Non-Conformity – NC*) sa zahtjevom u dvije razine
    a. velika (*major NC – NC MJ*)
    b. mala (*minor NC – NC MI*)
3. Prijedlog za poboljšanje (*Possible Improvements - PI*)
4. Neprimjenjivost zahtjeva sukladnosti na auditiran zahtjev (*Not Applicable N/A*)
5. Obrazloženje neprimjenjivosti zahtjeva (*Obrazloženje N/A*)
6. Obrazloženje prijedloga za poboljšanje (*Obrazloženje PI*)
7. Dokaz o pronalasku nesukladnosti ili dokumentirana informacija o sukladnosti sa zahtjevom (*Audit dokaz*)
8. Korektivna radnja (*Korektivna radnja u slučaju NC MJ i NC MI*)
9. Rok implementacije korektivne radnje (*Rok rješavanja u slučaju NC MJ i NC MI*)

Model se koristi na način da se tijekom provođenja analize stanja i/ili revizije sustava i/ili implementacije sustava informacijske sigurnosti i privatnosti ili usklađenosti s Uredbom i nacionalnim provedbenim zakonom redoslijedom prate postavljena audit pitanja i sukladno odgovorima na njih (usmenim/pisanim ispitivanjem unutarnjih i vanjskih dionika u organizaciji, anketom, testiranjem sustava, uvidom u dokumentaciju; ili u slučajevima kompleksnijih obrada kombinacijom svega navedenog) dodjeljuje klasifikacija ispunjenosti zahtjeva prema zadanim indikatorima. Zaključci uvijek moraju biti temeljeni na opservaciji sustava, razgovoru s dionicima i zaposlenicima, testiranju i analizi neophodne dokumentacije.

Sukladnost, odnosno usklađenost sa zahtjevom (*C*) dokazuje da su primijenjeni zahtjevi potpuno implementirani u sustav i učinkovit.

Nesukladnosti, odnosno neusklađenosti (*NC*) se klasificiraju velikima (*NC MJ*) kad postoji značajna sumnja da upravljanje procesima nije učinkovito i ne ispunjava zahtjev ili ako ukazuju na sustavnu grešku nizom manjih – povezanih ili nepovezanih, repetitivnih ili nerepetitivnih nesukladnosti koje je nužno rješavati u kratkom roku. Samostalne manje nesukladnosti (*NC MI*) su one koje ne utječu na sposobnost sustava upravljanja da postigne željene rezultate i nije ih neophodno rješavati u kratkom roku.

Prijedlozi za poboljšanje (*PI*) predstavljaju mjesta na kojima organizacija provodi određenu aktivnost sukladnu pojedinom zahtjevu no nije u mogućnosti dokumentirano ili dovoljno detaljno je dokazati na neki drugi način. Prijedlozi za poboljšanje ne predstavljaju nesukladnosti već preventivne radnje i označavaju mjesta na kojima se može unaprijediti trenutni proces kako njegovo trenutno stanje u budućnosti ne bi preraslo u nesukladnost.

Neprimjenjivost zahtjeva sukladnosti na zadan zahtjev (*N/A*) predstavlja stavku koju organizacija zbog prirode poslovanja nije u mogućnosti ispuniti ili je u definiranom opsegu sustava upravljanja organizacija nije uključila te prihvaća sve rizike koji iz tog isključenja proizlaze. Svaki neprimjenjiv zahtjev potrebno je detaljno obrazložiti (*obrazloženje N/A*). Ukoliko je obrazloženje činjenično utemeljeno, ono se prihvaća i evidentira kao takvo, dok u nedostatku činjenica koje dokazuju tu tvrdnju ono predstavlja nesukladnost.

Indikator prijedloga za poboljšanje također uvjetuje detaljno obrazloženje (*obrazloženje PI*) kako bi poslovodstvo moglo konkretno razmotriti doneseni prijedlog i planirati ili odbiti njegovu daljnju provedbu u svrhu unaprjeđenja sustava u vidu tog zahtjeva ili pristanka na postojeće stanje i daljnje praćenje tog statusa. Jedan od najvažnijih aspekata argumentiranog donošenja odluka o statusu pojedinih indikatora jest i transparentno evidentiranje prikupljenih dokaza (*audit dokaz*) kako bi se u slučaju revizije moglo brže doći do dokumentirane informacije o sukladnosti pojedinog zahtjeva ili pronalasku uzroka kod nastanka incidentnog događaja.

Korektivne radnje (*Korektivna radnja u slučaju NC MJ i NC MI*) predstavljaju aktivnosti koje organizacija po predmetnom zahtjevu planira napraviti kako bi otklonila uzrok nesukladnosti.

Rok implementacije korektivnih radnji (*Rok rješavanja u slučaju NC MJ i NC MI*) predstavlja konkretan brojčani vremenski pokazatelj planiranja potpunog otklanjanja pojedine nesukladnosti i najčešće je izražen datumom, te u rijetkim slučajevima brojem dana. Pokazatelj ovisi o razini nesukladnosti odnosno velike nesukladnosti (*NC MJ*) se moraju ukloniti što je prije moguće jer značajno utječu na sam sustav, dok se za male nesukladnosti (*NC MI*) može definirati širi vremenski aspekt.

Model je temeljen na analizi indikatora slijedom audit pitanja vezanih uz zahtjeve i smjernice standarda informacijske sigurnosti i privatnosti te analizi rizika u međudjelovanju triju faktora – poznavanjem informacijske imovine organizacije uključivši postojeće prijetnje i ranjivosti sustava, regulatornih obveza i odnosa klasifikacije nesukladnosti s rokovima njihovog uklanjanja. Pri određivanju opsega važno je napomenuti da se stavke koje utječu na funkcionalnost sustava u smislu održavanja trijade informacijske sigurnosti ne mogu proglasiti neprimjenjivima. Trijada na kojoj počiva svrha ovih standarda, kao i zakonodavstva vezanog uz zaštitu podataka, podrazumijeva točnost, cjelovitost i dostupnost podataka (uključivši i osobne podatke).

Način korištenja modela metodološki je prilagođen načinu izvođenja internog audita odnosno audita prve strane, te audita druge strane.

Tablica 13. – Različite vrste audita prema ISO 19011

Audit prve strane	Audit druge strane	Audit treće strane
Interni audit	Audit od strane vanjskog pružatelja usluge	Certifikacijski i/ili akreditacijski audit
	Audit od strane ostalih vanjskih zainteresiranih strana	Zakonska, regulatorna ili slična revizija

Izvor: ISO 19011, ISO

Samo upravljanje rizicima je (Sabolić, 2013) proces identifikacije, procjene i prioritizacije rizika, uz ekonomičnu i koordiniranu primjenu resursa u minimizaciju rizika, nadzoru i upravljanjem tim neizvjesnim događajima u smislu evaluacije njihove vjerojatnosti i intenziteta učinka. Spremić (2017) je kod upravljanja rizicima napomenuo da najteži dio procesa predstavlja njihova identifikacija i klasifikacija u smislu pregleda prijetnji, slabosti sustava i očekivanih negativnih učinaka te određivanja vjerojatnosti nastanka, kao i dodjeli odgovornosti za sam rizik.

Najčešće tehnike prikupljanja podataka radi identifikacije razine ispunjavanja zahtjeva i smjernica su anketni upitnici, razgovori s dionicima u organizaciji (internim i eksternim), pregled dokumentacije i opservacija rada samog sustava. Pri korištenju modela opseg samog sustava u organizaciji ovisit će o protoku osobnih podataka u organizaciji te će zapravo identifikacija tog indikatora posljedično (u najvećem broju slučajeva) proširiti prvotno definiran opseg ukoliko je on od početka procesa bio planiran u smanjenom opsegu.

Tablica 14. – Metode auditiranja prema ISO 19011

Opseg uključenosti između revizora i subjekta revizije	**Lokacija auditora**	
	Neposredno	**Na daljinu**
Interakcija među ljudima	Provođenje intervjua Popunjavanje kontrolnih popisa i upitnika uz sudjelovanje ispitanika Provođenje pregleda dokumentacije uz sudjelovanje ispitanika Uzorkovanje	Kroz interaktivnu komunikaciju znači: - vođenje razgovora; - promatranje obavljanja posla korištenjem daljinskog vodiča; - popunjavanje kontrolnih lista i upitnika; - provođenje pregleda dokumentacije uz sudjelovanje ispitanika.
Bez interakcije među ljudima	Provođenje pregleda dokumentacije (npr. zapisi, analiza podataka) Promatranje obavljanja posla Provođenje posjeta na licu mjesta Popunjavanje kontrolnih popisa Uzorkovanje (npr. proizvodi)	Provođenje pregleda dokumentacije (npr. zapisi analiza podataka) Promatranje obavljanja posla korištenjem nadzornih sredstava, uzimajući u obzir socijalne i zakonske i regulatorne zahtjeve Analiziranje podataka
Aktivnosti neposrednog audita obavljaju se u mjestu auditirane osobe. Aktivnosti audita na daljinu izvode se na bilo kojem mjestu, osim na mjestu na kojem se nalazi auditirana osoba, bez obzira na udaljenost. Interaktivne audit aktivnosti uključuju interakciju između osoblja auditirane osobe i audit tima. Neinteraktivne audit aktivnosti ne uključuju ljudsku interakciju s pojedincima koji predstavljaju auditiranu osobu, ali uključuju interakciju s opremom, objektima i dokumentacijom.		

Izvor: ISO 19011, ISO

4.3.1. Ekspertna znanja u provođenju analize ili revizije

Preporučljivo je da stručnjak odnosno auditor[69] koji će provoditi analizu organizacije temeljem zadanog modela posjeduje određene minimalne kompetencije ovisne o opsegu posla za koji je zadužen ili moguću postojeću dužnost koju obnaša, a vezana je uz ISO standarde.

Interni auditor je osoba koja je u najvećem broju slučajeva zaposlenik organizacije ili vanjska osoba koja je u potpunosti upoznata s procesima unutar organizacije, njezinom strukturom kao i organizacijskim i tehničkim aspektima koje ima na raspolaganju. Vodeći auditor (*lead auditor*) je osoba koja u pravilu posjeduje akreditirani certifikat razine *lead auditora* za dužnost auditiranja koju obnaša te je može auditirati organizacijske i tehničke mjere te usklađenost sa standardima i zakonskom regulativom, za što posjeduje stručna znanja, u više različitih organizacija iz različitih sektora djelovanja. Akreditirani certifikacijski auditor je osoba koja za i u ime certifikacijske kuće provodi audite te izvještava organizaciju i certifikacijsku kuću o nalazima vezanim uz usklađenost sa standardom za koji se organizacija certificira i/ili predmetnom pravnom regulativom koju pojedini standard uvjetuje (standardi informacijske sigurnosti, kao i velik broj drugih standarda propisuju obvezu usklađenosti sa pravnom regulativom iz tog područja). U slučajevima kad certifikacijski auditor ne posjeduje dovoljna znanja o pravnoj regulativi ili drugoj specifičnosti industrije organizacije vezanoj uz predmetni standard za koji je akreditiran, certifikacijska kuća osigurava dodatnu osobu na samom auditu, odnosno eksperta za pojedino područje.

Za korištenje izloženog modela u pojedinoj zemlji potrebno je detaljno razumijevanje Opće uredbe o zaštiti podataka i nacionalnog provedbenog zakona zemlje te je preporučljiva minimalna razina edukacije, odnosno edukacije za internog auditora standarda ISO/IEC 27001 i ISO/IEC 27701.

U slučajevima kad osoba koja provodi audit korištenjem ovog modela, isto radi za različite organizacije iz različitih sektora djelovanja i pravnih regulativa, preporučljivo je posjedovanje

[69] Auditor odnosno revizor – osoba koja prikuplja i obrađuje podatke prema zadanom opsegu i klasifikaciji te sudjeluje u procjeni ili samostalno procjenjuje usklađenost pojedinog zahtjeva ili smjernice sukladno zadanoj klasifikaciji nakon čega zaključno daje svoje mišljenje bazirano na dokumentiranim i objektivnim argumentima na daljnje postupanje.

certifikata vodećeg auditora za standarde ISO/IEC 27001 i ISO/IEC 27701, a organizacijama je preporučeno da istu razinu minimalnih kompetencija stručnjaka uvjetuju stjecanjem navedenih certifikata prije angažiranja stručnjaka za tu vrstu usluga.

Certifikacijski auditori mogu ovim modelom provoditi procjene učinkovitosti i razine implementiranosti sustava upravljanja informacijskom sigurnošću i privatnošću i/ili usklađenosti tehničkih i organizacijskih mjera s Uredbom i nacionalnim provedbenim zakonom ako ne obnašaju dužnost certifikacijskog auditora u istoj organizaciji prilikom certifikacijskog ili nadzornog audita od strane certifikacijske kuće u vremenu definiranom ugovornim odredbama o izbjegavanju sukoba interesa svake pojedine certifikacijske kuće.

Pri izvođenju certifikacijskog audita i korištenja ovog modela kao audit upitne liste, model se može koristiti za procjenu usklađenosti sa zahtjevima standarda, uz sve ostale obveze u provedbama audita od strane certifikacijskih tijela propisane standardom ISO/IEC 17021-1[70]

4.3.2. Certifikacija

Za potvrdu usklađenosti s Uredbom u ovom trenutku ne postoji odobrena procedura ili certifikacija od strane Europske komisije. No na tržištu već postoji certifikacija ISO/IEC 27001 sustava upravljanja informacijskom sigurnošću s opsegom proširenim na ISO/IEC 27701 sustav upravljanja privatnošću. Jedan od prvih takvih certifikata jest Microsoftov[71], koji je ovako integriranim sustavom akreditirano certificirao sve svoje *Azure* servise kako bi svojim klijentima pokazao pozitivan smjer i dokaz visoke razine sigurnosti podataka u aspektima organizacijskih i tehničkih mjera vezanih uz usklađenost s Uredbom.

[70] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2015). *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements* (ISO/IEC 17021-1)
[71] Burt, D. (2020) *Azure is now certified for the ISO/IEC 27701 privacy standard*. Microsoft. Dostupno na: https://azure.microsoft.com/en-us/blog/azure-is-now-certified-for-the-iso-iec-27701-privacy-standard/, pristupljeno 17.1.2021.

Prema Tunjić et al (2016) tvrtka koja nije certificirala svoje sustave i prošla neovisni audit treće strane, nema stvarnu ocjenu cjelokupnog sustava upravljanja koje uvodi, a kojom konačno završava ciklus uvođenja pojedinog sustava te ističe i da certifikat značajno utječe na jačanje ugleda tvrtke u javnosti, na tržištu, kao i na konkurentsku sposobnost tvrtke.

Važno je napomenuti da standard ISO/IEC 27701 predstavlja ekstenziju odnosno dopunu zahtjeva i kontrola standarda ISO/IEC 27001 u proširenju zahtjeva i kontrola vezanih uz prikupljanje, obradu i arhiviranje osobnih podataka te predstavlja skup organizacijskih i tehničkih mjera koje organizacija mora ispuniti ili obrazložiti izuzeće od pojedine stavke, a koje ne utječe na funkcionalnost sustava kao takvog. S tim u svezi, ovaj standard nije moguće samostalno akreditirano certificirati odnosno izdvojeno od ISO/IEC 27001 certifikacije. Akreditacijsko tijelo UKAS u ožujku 2020. godine iznijelo je smjernice[72] certifikacijskim kućama za akreditaciju proširenja ovlasti auditiranja i izdavanja akreditiranih certifikata standarda ISO/IEC 27001 na opseg ISO/IEC 27001 s uključenim ISO/IEC 27701 koje potvrđuje tu tvrdnju.

4.4. Verifikacija modela

Verifikacija modela je provedena na uzorku od pet poduzeća te je potvrđeno da dobiveni procesni model zadovoljava postavljene specifikacije, odnosno da organizacijama olakšava razumijevanje zahtjeva propisanih Općom uredbom o zaštiti podataka i implementiranje tehničkih i organizacijskih mjera u skladu s ovom zakonskom regulativom, kao i implementiranje i reviziju sustava upravljanja ISO/IEC 27001 i njegove ekstenzije. Rezultati vrednovanja modela potvrđuju da je primjenom predložene metode ostvaren aplikativni doprinos.

[72] UKAS (2020). *Technical Bulletin: ETS ISO/IEC 27701:2019, ISO/IEC 27001 & ISO/IEC 27002*. Dostupno na. https://www.ukas.com/resources/technical-bulletins/technical-bulletin-guidance-on-applying-for-an-extension-to-scope-for-iso-iec-277012019-extension-to-iso-iec-27001-and-iso-iec-27002-for-privacy-information-management/, pristupljeno 17.01.2021.

Predloženi se model temelji na međunarodnim standardima koji su dinamičke norme, koje se u nespecificiranom vremenu obnavljaju i poboljšavaju, pa je model uputno revidirati i usklađivati s njihovim izmjenama ako se njime služi radi implementacije i certifikacije sustava upravljanja informacijske sigurnosti i privatnosti te u slučaju promjena vezanih uz Opću uredbu o zaštiti podataka i propisanih organizacijskih i tehničkih mjera.

Model je testiran u ukupno pet poduzeća iz različitih sektora: farmaceutskog sektora, sektora proizvodnje kozmetičkih proizvoda, IKT sektora, zdravstvenog sektoru i sektora hotelijerstva. Tri su poduzeća imala 21–50, a dva 20 i manje zaposlenika. U dva poduzeća s 21-50 zaposlenika model je testiran uz pomoć konzultanta za zaštitu osobnih podataka, a u ostala je tri poduzeća testiran samostalno. Samostalno su korištenje proveli zaposlenici vezani uz marketing, IKT i pravne odnose (interni pravni odjel ili eksterne pravne usluge). Vrsta osobnih podataka, njihova obrada i dijeljenje s trećim stranama kretala se od jednostavne do kompleksne, pri čemu je kompleksna podrazumijevala i elektroničku razmjenu osobnih podataka s trećim stranama u trećim zemljama te korištenja programa lojalnosti, praćenja napretka ili navika ispitanika i ostalih marketinških metoda temeljenih na profiliranju. Sva su poduzeća bila u svojstvu i voditelja i izvršitelja obrade, ovisno o pojedinoj identificiranoj obradi i njezinoj svrsi.

Nakon usklađivanja poduzeća korištenjem ovog modela, nad svim je poduzećima izveden kontrolni audit od strane dvaju neovisnih certificiranih *lead auditora* s višegodišnjim iskustvom u provedbi internih audita, audita druge strane i audita treće strane sustava upravljanja informacijskom sigurnošću.

Razdoblje korištenja modela u usklađivanju predmetnih poduzeća započelo je u srpnju 2020. godine, a završilo krajem prosinca 2020. godine. Neovisni kontrolni audit druge strane izveden je po završetku implementacije usklađenosti korištenjem modela od strane svakog pojedinog poduzeća te je rezultirao detaljnim izvješćem s brojčano iskazanom količinom razlika u pronalascima i opisom pronalazaka obaju kontrolnih auditora, s posebnom pažnjom usmjerenom na identifikaciju mogućeg nerazumijevanja sadržaja pojedinog pitanja u modelu ili načina klasifikacije pojedine opcije odnosno C, NC MJ, NC MI, N/A, obrazloženja N/A, PI, obrazloženja PI, audit dokaza, korektivnih radnji te njihovog roka rješavanja.

Izvedba kontrolnih audita napravljena je tako da nijedan neovisni auditor nije bio upućen u sadržaj auditorskih pronalazaka drugog auditora. U svrhu istraživanja i verifikacije modela, poduzećima je osigurana povjerljivost podataka na način da su i autorica i oba neovisna auditora potpisali sporazum o dvostrukoj povjerljivosti (*Non-Disclosure Agreement – NDA*) te im je zajamčena potpuna anonimnost. Zbog moguće identifikacije poduzeća uslijed objave izvješća s kontrolnih audita, iskazani su njihovi agregirani rezultati.

Na kraju siječnja 2021. zaprimljeno je ukupno 10 detaljnih izvješća s kontrolnih audita, po dva za svako poduzeće. Nisu pronađene razlike u kontrolnim auditima pojedinih poduzeća između izvješća dvaju neovisnih auditora, što predstavlja verifikaciju metodologije modela s ciljem auditiranja usklađenosti organizacijskih i tehničkih mjera s Uredbom, odnosno usklađenosti sa kontrolama standarda ISO/IEC 27001 i njegovom ekstenzijom odnosno standardom ISO/IEC 27701.

U izvješćima kontrolnih audita nije pronađen nalaz koji bi upućivao na to da postoji viši stupanj razumijevanja korištenja modela kod poduzeća koje su ga sama koristila u odnosu na poduzeća koja su ga koristila uz pomoć konzultanata, iako je proces usklađivanja u poduzećima u kojima je korišten samostalno bio nešto duži, no pritom se ne može isključiti izražena sezonalnost u povećanju ili smanjenju opsega samog poslovanja pojedinih poduzeća tijekom ljetnih mjeseci kao razlog dužeg usklađivanja.

Poduzeća su bila detaljno upućena u način korištenja modela, objašnjena im je terminologija i metodološka logika međunarodnih ISO standarda temeljenih na PDCA ciklusu.

Sva su poduzeća u cijelosti ispunila audit upitnu listu, odnosno klasificirali su usklađenost vlastitih organizacijskih i tehničkih mjera sukladno predloženoj klasifikaciji, identificirali područja za poboljšanje, procijenili primjenjivost pojedinog zahtjeva s obzirom na postojeće procese, obrazložili moguću neprimjenjivost zahtjeva, evidentirali audit dokaze i korektivne mjere u slučaju nesukladnosti te predložili rokove za njihovo otklanjanje.

Kontrolni se audit sastojao od dvostrukog dubinskog snimanja procesa i evidentiranja nalaza sukladno standardima i korištenjem primijenjenog modela te su dobiveni rezultati potom

sadržajno uspoređeni s rezultatima primjene modela, provedene samostalno ili uz pomoć konzultanata.

Uspoređeni su rezultati ukazali na to da su poduzeća i konzultanti gotovo u potpunosti razumjeli sadržaj audit pitanja i svoje obveze po ispunjenju zahtjeva vezanih uz organizacijske i tehničke mjere propisane Uredbom, pravilno su identificirali sukladnost u odnosu na nesukladnost, primjenjivost pojedinih zahtjeva, uočili nesukladnost i ispravno zadali rokove za rješavanje nesukladnosti te evidentirali dokaze pri ispunjavanju primjenjivih zahtjeva navedenih u modelu u skladu s postojećim procesima u poslovanju.

Oba su neovisna auditora prilikom kontrolnog audita u jednom poduzeću identificirali nedostatnost u definiranju pravnog statusa kod obrade osobnih podataka koja uključuje angažman treće strane, a koja je u izvješću klijenta pogrešno evidentirana. Nedostatnost se manifestirala u aspektu pogrešno definiranih odgovornosti i obveza treće strane koja nije bila u svojstvu izvršitelja obrade već voditelja obrade u izdvojenoj aktivnosti obrade osobnih podataka.

5. NPISPMSA model[73]

Procjena usklađenosti organizacijskih i tehničkih mjera sa zahtjevima Kontrola A ISO/IEC 27001:2013, ISO/IEC 27002:2013 te zahtjevima ISO/IEC 27701:2019, Uredbe i nacionalnog provedbenog zakona										
A.5 ISMS										
A.5.1 ISMS										
A.5.1.1 ISMS / PIMS 6.2.1.1	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su politike vezane uz informacijsku sigurnost definirane, odobrene od poslovodstva, objavljene i prenesene svim zaposlenicima i relevantnim vanjskim stranama?										
Da li je organizacija u sklopu politika informacijske sigurnosti ili izdvojenih politika o privatnosti sastavila izjavu vezanu uz svoje podržavanje i predanost ostvarenju usklađenosti s primjenjivom legislativom/regulativom vezanom uz zaštitu osobnih podataka?										

[73] Izvedeno iz standarda: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2019). *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (ISO/IEC 27701:2019)*; International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2013). *Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013)*; International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2013). *Information technology — Security techniques — Code of practice for information security controls (ISO/IEC 27002:2013)* i mapirano s nacionalnim provedbenim zakonom (*Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18))*

Da li ta izjava sadržava i stavke vezane uz ugovorne uvjete između organizacije i njezinih partnera, podugovoritelja i ostalih trećih strana (klijenti, dobavljači i slično) te su u njoj jasno raspodijeljene odgovornosti među njima?										
A.5.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se politike vezane uz informacijsku sigurnost pregledavaju u planiranim intervalima ili u slučaju značajnih promjena, kako bi se osigurala njihova trajna prikladnost, primjerenost i djelotvornost?										
A.6 ISMS										
A.6.1 ISMS										
A.6.1.1 ISMS / PIMS 6.3.1.1	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su definirane i pridijeljene sve odgovornosti za informacijsku sigurnost u organizaciji?										
Da li je organizacija postavila kontaktnu osobu za klijenta u odnosima koji su vezani uz obradu osobnih podataka?										

	U slučajevima kad je organizacija u svojstvu voditelja obrade, da li je postavila i kontakt osobu za ispitanike, a vezano uz obradu njihovih osobnih podataka?										
	Da li je organizacija provela procjenu obveze imenovanja Službenika za zaštitu podataka?										
	Da li je organizacija obveznik imenovanja Službenika za zaštitu podataka?										
	Ukoliko je organizacija obveznik imenovanja Službenika za zaštitu podataka, da li je ta pozicija podugovorena s trećom stranom?										
	Da li je organizacija imenovala jednu ili više odgovornih osoba odgovornih za razvoj, uvođenje, održavanje i nadzor programa za upravljanje informacijama o privatnosti koji pokriva cijelu organizaciju u svrhu usklađenosti sa svim primjenjivih legislativama i regulativama vezanim uz zaštitu osobnih podataka?										
	Da li je imenovana odgovorna osoba nezavisna i omogućeno joj je direktno izvještavanje odgovarajuće razine rukovodstva organizacije zaduženog za upravljanje rizicima vezanim uz privatnost?										
	Da li je imenovana odgovorna osoba uključena u rukovođenje svim predmetima koji se odnose na obradu osobnih podataka?										
	Da li je imenovana odgovorna osoba dovoljno kompetentna u aspektima legislative, regulative i prakse vezane uz zaštitu podataka?										

Da li je imenovanoj odgovornoj osobi definirano i zaduženje djelovanja kontaktne osobe za nadležna nadzorna tijela?										
Da li imenovana odgovorna osoba ima definirano i zaduženje obavještavanja najviše razine rukovodstva organizacije i zaposlenika o njihovim obvezama vezanim uz obrade osobnih podataka, te da li joj je dodijeljena i savjetodavna funkcija u slučajevima kad organizacija provodi procjene utjecaja na privatnost?										
A.6.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija razdijelila proturječne dužnosti i područja odgovornosti u svojstvu smanjenja prilika za neovlaštenu ili nenamjernu modifikaciju ili zlouporabu organizacijske imovine?										
A.6.1.3 ISMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija identificirala Agenciju za zaštitu osobnih podataka (AZOP) kao nadležno tijelo sukladno nacionalnom provedbenom zakonu?										

Da li organizacija održava primjerene kontakte s drugim nadležnim tijelima po potrebi?										
A.6.1.4 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija održava kontakte s posebnim interesnim grupama ili drugim specijalističkim sigurnosnim forumima i profesionalnim udruženjima?										
A.6.1.5 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija uključila informacijsku sigurnost u upravljanju svim projektima?										
A.6.2 ISMS										
A.6.2.1 ISMS / PIMS 6.3.2.1	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija usvojila politiku mobilnih uređaja i potporne sigurnosne mjere?										

Da li je organizacija osigurala da korištenje mobilnih uređaja ne dovodi do ugrožavanja osobnih podataka?										
A.6.2.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su politika rada na daljinu i potporne sigurnosne mjere implementirane kako bi se zaštitile informacije kojima se pristupa, obrađuje ili pohranjuje na lokacijama predviđenim za rad na daljinu?										
A.7 ISMS										
A.7.1 ISMS										
A.7.1.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija provodi sigurnosnu provjeru svih kandidata za zapošljavanje u skladu s važećim zakonima, propisima i etikom te da li je ona razmjerna poslovnim zahtjevima, klasifikacijom informacija kojima će se pristupati te prepoznatim rizicima?										

A.7.1.2 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li su u ugovorima sa zaposlenicima i drugim ugovornim stranama navedene njihove odgovornosti i odgovornosti organizacije po pitanju informacijske sigurnosti?										
A.7.2 ISMS										
A.7.2.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li poslovodstvo zahtijeva da svi zaposlenici i druge ugovorne strane primjenjuju informacijsku sigurnost u skladu s uspostavljenim politikama i procedurama unutar organizacije?										
A.7.2.2 ISMS / PIMS 6.4.2.2	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li svi zaposlenici organizacije i, gdje je relevantno, druge ugovorne strane, moraju proći primjerenu edukaciju i osposobljavanje o svjesnosti te redovito upoznavanje s promjenama politika i procedura organizacije koje su relevantne za njihovu poslovnu funkciju?										
Da li su uvedene i mjere, uključujući i svjesnost o izvještavanju o incidentima, kojima je osigurano da je odgovarajuće osoblje svjesno mogućih posljedica za organizaciju poput pravnih posljedica, gubitka reputacije i slično, posljedica po člana osoblja poput disciplinskih mjera te posljedica za ispitanike u aspektima fizičkih, materijalnih i duševnih posljedica uslijed kršenja pravila i procedura vezanih uz privatnost ili sigurnost, a osobito onih koji se odnose na postupanje s osobnim podatcima?										
Da li organizacija provodi odgovarajuće povremene edukacije za osoblje koje ima pristup osobnim podatcima u sustavu?										
A.7.2.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je uveden i prenesen formalni disciplinski proces za poduzimanje radnji protiv zaposlenika koji su počinili kršenje u aspektima informacijske sigurnosti?										
A.7.3 ISMS										

A.7.3.1 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li su odgovornosti i zaduženja vezana uz informacijsku sigurnost koje ostaju važeće i nakon prekida ili promjene zaposlenja definirane i prenesene zaposleniku ili drugoj ugovornoj strani te da li se provode?										
A.8 ISMS										
A.8.1 ISMS										
A.8.1.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je imovina povezana s informacijama i opremom za obradu informacija definirana te postoji li popis redovito ažuriran popis te imovine?										
A.8.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li popis imovine sadrži i vlasnika imovine?										
A.8.1.3 ISMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su pravila za prihvatljivo korištenje informacija i imovine povezane s informacijama i opremom za obradu informacija identificirana, dokumentirana i implementirana?										
Da li je organizacija sustav pohrane snimaka prikupljenih videonadzorom evidentirala dijelom informacijske imovine sukladno, uz ostalo, i svim zahtjevima propisanim nacionalnim provedbenim zakonom?										
Da li je organizacija u slučaju da koristi sustav obrade biometrijskih podataka osigurala da je to u skladu, uz ostalo, i sa zahtjevima propisanim nacionalnim provedbenim zakonom?										
U slučaju da organizacija koristi sustave obrade biometrijskih podataka u svrhe evidentiranja radnog vremena te ulaska i izlaska iz službenih prostorija, a ukoliko za to ne postoji zakonska obveza, da li je osigurala i alternativno rješenje sukladno nacionalnom provedbenom zakonu?										
A.8.1.4 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li svi zaposlenici i korisnici trećih strana nakon prekida zaposlenja, ugovora ili sporazuma vraćaju svu imovinu organizacije koja je do tada bila u njihovom posjedu?										
A.8.2 ISMS										
A.8.2.1 ISMS / 6.5.2.1 PIMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su informacije klasificirane u okvirima zakonskih zahtjeva, vrijednosti, kritičnosti i osjetljivosti na neovlašteno otkrivanje ili izmjene?										
Da li sustav klasifikacije informacija eksplicitno razmatra i pojam osobnih podataka kao dio implementirane sheme?										
Da li je identificirano koje vrste i kategorije osobnih podataka organizacija obrađuje, gdje su oni čuvani i kojim sve sustavima protječu?										
U slučaju da koristi videonadzor, da li je organizacija informacije prikupljene sustavom videonadzora propisno klasificirala te uzela u obzir, uz ostalo, i zahtjeve nacionalnog provedbenog zakona?										
U slučaju da koristi sustave biometrijske obrade podataka da li je organizacija informacije prikupljene tim sustavom propisno klasificirala										

te uzela u obzir, uz ostalo, i zahtjeve nacionalnog provedbenog zakona?										
A.8.2.2 ISMS / 6.5.2.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je razvijen prikladan skup procedura za označavanje informacija i da li je primijenjen u skladu s usvojenom klasifikacijskom shemom informacija?										
Da li je organizacija osigurala da su ljudi pod njenom jurisdikcijom svjesni definicije osobnog podatka i načina na koji će prepoznati informaciju koja predstavlja osobni podatak?										
A.8.2.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su procedure za rukovanje imovinom razvijene i primijenjene u skladu s usvojenom klasifikacijskom shemom?										
A.8.3 ISMS										

A.8.3.1 ISMS / 6.5.3.1 PIMS / NPZ	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li su procedure za upravljanje uklonjivim medijima primijenjene u skladu s usvojenom klasifikacijskom shemom?										
Da li organizacija posjeduje dokumentiranu informaciju o korištenju uklonjivih medija i/ili uređaja koje koristi za pohranu osobnih podataka?										
Da li organizacija šifrira odnosno kriptira uklonjive fizičke medije i/ili uređaje prilikom pohrane osobnih podataka?										
U slučaju da organizacija nema mogućnost šifriranja odnosno kriptiranja medija za pohranu osobnih podataka, da li je implementirala postupke i kompenzacijske kontrole kako bi smanjila rizike vezane uz ophođenje s njima?										
Da li je organizacija u slučaju korištenja videonadzora sa sustavom pohrane uzela u obzir rok čuvanja te vrste podataka s obzirom na zahtjeve propisane, uz ostalo, i nacionalnim provedbenim zakonom?										
A.8.3.2 ISMS / 6.5.3.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li postoje i provode se formalne procedure za odbacivanje nepotrebnih medija koje osiguravaju njihovo uklanjanje na siguran način?										
Da li su pri uklanjanju medija za koje postoji mogućnost da sadrže i osobne podatke implementirane sigurnosne procedure u svojstvu osiguravanja da takvi podatci više ne mogu učiniti dostupnima te da li su takve procedure dokumentirane?										
A.8.3.3 ISMS / 6.5.3.3 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su mediji koji sadrže informacije zaštićeni od neovlaštenog pristupa, zloupotrebe ili oštećenja tijekom transporta?										
Da li u slučaju korištenja fizičkih medija za pohranu osobnih podataka postoji sustav evidentiranja njihovih ulaznih i izlaznih aktivnosti koji uključuje informacije o vrsti fizičkog medija, osobi ovlaštenoj za slanje/primanje te datum, vrijeme i broj fizičkog medija.										
Da li su osigurane i dodatne mjere poput šifriranja odnosno kriptiranja da se podatcima može pristupiti samo na njihovom odredištu, a ne i prilikom tranzita?										

Da li je dešifriranje odnosno dekriptiranje medija za koje je moguće da sadrže osobne podatke ograničeno samo na ovlašteno osoblje?										
A.9 ISMS										
A.9.1 ISMS										
A.9.1.1 ISMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je politika kontrole pristupa utemeljena na poslovnim zahtjevima i zahtjevima informacijske sigurnosti uspostavljena, dokumentirana i pregledana?										
U slučaju da organizacija koristi videonadzor, da li je organizacija utvrdila odgovornu osobu odnosno osobu ovlaštenu za pristup podatcima na tom sustavu pohrane, te je u mogućnosti osigurati da pristup njemu imaju imaju i, sukladno nacionalnom provedbenom zakonu, po potrebi nadležna državna tijela u okviru obavljanja poslova iz svojeg zakonom utvrđenog djelokruga?										
A.9.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li je korisnicima omogućen pristup samo onim mrežama i mrežnim uslugama za čije korištenje su posebno ovlašteni?										
A.9.2 ISMS										
A.9.2.1 ISMS / 6.6.2.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Postoji li formalni proces registracije i de-registracije korisnika pri dodjeli prava pristupa?										
Da li je u procedurama za registraciju i de-registraciju korisnika koji administriraju ili upravljaju sustavima i uslugama koji obrađuju osobne podatke definiran postupak u slučaju kompromitirane kontrole korisničkog pristupa za te korisnike?										
Postoji li sustav automatiziranog izdavanja korisničkih pristupa kako bi se preveniralo ponovno izdavanje deaktiviranih ili isteklih korisničkih imena za sustave i usluge koji obrađuju osobne podatke?										
Postoje li dokumentirane informacije u slučajevima kada organizacija pruža usluge vezane uz obrade osobnih podataka, a u kojima je klijent odgovoran za neke ili sve aspekte upravljanja korisničkim imenom?										

Da li je organizacija identificirala moguće specifične zahtjeve zakonodavstva unutar kojeg djeluje, vezane uz učestalost provjere nekorištenih podataka za ovjeru vjerodostojnosti (autorizaciju) nad sustavima koji obrađuju osobne podatke te se uskladila s njima?										
A.9.2.2 ISMS / 6.6.2.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se formalni proces dodjeljivanja korisničkog pristupa primjenjuje pri dodjeli ili opozivu prava pristupa za sve vrste korisnika i na sve sustave i usluge?										
Da li organizacija održava točnu i ažuriranu evidenciju korisničkih profila kreiranih za korisnike kojima je odobren pristup informacijskom sustavu i pohranjenim osobnim podatcima?										
Da li takva evidencija obuhvaća i podatke o korisniku, uključujući korisničko ime potrebno za implementaciju kontrola tehničke identifikacije koje omogućuju povlašteni pristup, a kojima se u svakom trenutku može ustanoviti tko je pristupio osobnim podatcima te što je dodano, izbrisano ili izmijenjeno?										

Posjeduje li organizacija dokumentirane informacije o načinima na koje je klijentima pružila mogućnost upravljanja pristupom bilo da se radi o osiguravanju prava na administraciju sustava ili prekidanje pristupa, u slučaju kad organizacija pruža usluge obrade osobnih podataka i klijent je odgovoran za neke ili sve aspekte upravljanja tim pristupom?										
A.9.2.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je pridjeljivanje i korištenje povlaštenih prava pristupa ograničeno i strogo kontrolirano?										
A.9.2.4 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je pridjeljivanje tajnih autentifikacijskih informacija strogo kontrolirano putem formalnog upravljačkog procesa?										
A.9.2.5 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li vlasnici imovine pregledavaju korisnička prava pristupa u redovitim intervalima?										

A.9.2.6 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se prava pristupa informacijama i opremi za obradu informacija zaposlenicima i korisnicima vanjskih strana ukidaju pri prekidu njihova zaposlenja, ugovora ili sporazuma, ili se prilagođavaju nakon svake promjene njihovog statusa?										
A.9.3 ISMS										
A.9.3.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se od korisnika zahtijeva pridržavanje organizacijskih praksi pri korištenju tajnih autentifikacijskih informacija?										
A.9.4 ISMS										
A.9.4.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li je pristup informacijama i funkcijama aplikacijskog sustava ograničen i u skladu s politikom kontrole pristupa?										
A.9.4.2 ISMS / 6.6.4.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je kod zahtjeva vezanog uz politiku kontrole pristupa, pristup sustavima i aplikacijama kontroliran procedurom sigurnog prijavljivanja (log-on)?										
Da li organizacija može klijentu na njegov zahtjev omogućiti sigurno prijavljivanje (log-on) za svaki korisnički račun kojeg on kontrolira?										
A.9.4.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su sustavi za upravljanje zaporkama interaktivni i osiguravaju kvalitetne zaporke?										
A.9.4.4 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li je korištenje uslužnih programa koji mogu biti sposobni zaobići kontrole sustava ograničeno i strogo kontrolirano?										
A.9.4.5 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je pristup izvornom kodu programa ograničen?										
A.10 ISMS										
A.10.1 ISMS										
A.10.1.1 ISMS / 6.7.1.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je razvijena i primijenjena politika korištenja kriptografskih kontrola?										
Da li je organizacija identificirala postoji li pravna obveza, s obzirom na obvezujuću regulativu, korištenja kriptografije za zaštitu određene vrste osobnih podataka poput zdravstvenih podataka, matičnih brojeva rezidenata, osobnih dokumenata i slično?										

Može li organizacija klijentima pružiti informaciju o okolnostima u kojima koristi kriptografiju u zaštiti osobnih podataka koje obrađuje?										
Može li organizacija klijentima pružiti informaciju o bilo kakvim mogućnostima koje ima na raspolaganju, a koje bi im mogle poslužiti u postavljanju njihove vlastite kriptografske zaštite?										
A.10.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je politika korištenja, zaštite i vijeka trajanja kriptografskih ključeva razvijena i primijenjena na njihov cijeli životni ciklus?										
A.11 ISMS										
A.11.1 ISMS										
A.11.1.1 ISMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su definirani sigurnosni parametri i koriste se kako bi se zaštitila područja koja sadrže osjetljive ili kritične informacije i opremu za obradu informacija?										

Da li je organizacija u slučaju korištenja videonadzora, kod definiranja perimetra snimanja, uzela u obzir ograničenja propisana i nacionalnim provedbenim zakonom?										
Da li je organizacija u slučaju korištenja videonadzora, uzela u obzir zahtjev o obavješćivanju ispitanika o ulasku u perimetar snimanja i osigurala mu sve obvezne informacije na način propisan nacionalnim provedbenim zakonom?										
A.11.1.2 ISMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su sigurnosna područja zaštićena odgovarajućim kontrolama ulaza kako bi se osiguralo da je pristup dopušten samo ovlaštenom osoblju?										
Da li je organizacija u slučaju korištenja sustava biometrijske obrade podataka ili videonadzora u fizičkoj kontroli ulaza uzela u obzir ograničenja propisana, uz ostalo, i nacionalnim provedbenim zakonom?										
A.11.1.3 ISMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je definirana i primijenjena fizička sigurnost za urede, prostorije i opremu?										

Da li je organizacija u slučaju korištenja sustava videonadzora u svojstvu osiguravanja fizičke sigurnosti za urede, prostorije i opremu, uzela u obzir ograničenja perimetra snimanja propisana, uz ostalo, i nacionalnim provedbenim zakonom?										
A.11.1.4 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je definirana i primijenjena fizička zaštita protiv prirodnih katastrofa, zlonamjernih napada ili nezgoda?										
A.11.1.5 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su definirane i primijenjene procedure za rad u sigurnim područjima?										
A.11.1.6 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su pristupne točke poput područja za isporuku, utovar i slično, na kojima bi neovlaštene osobe mogle ući u prostorije strogo kontrolirane i, ako je moguće, izolirane od										

opreme za obradu informacija kako bi se spriječio neovlašteni pristup?										
A.11.2 ISMS										
A.11.2.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je oprema smještena ili zaštićena kako bi se smanjio rizik od prijetnji i opasnosti okoline te smanjile prilike za neovlašten pristup?										
A.11.2.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je oprema zaštićena od energetskih kvarova i ostalih prekida uzrokovanih prekidima potpornih komunalnih usluga?										
A.11.2.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li su energetski i telekomunikacijski kablovi koji prenose podatke ili su potpora informacijskim uslugama zaštićeni od presretanja prometa, ometanja ili oštećenja?										
A.11.2.4 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se oprema pravilno održava kako bi se osigurala njena kontinuirana raspoloživost i cjelovitost?										
A.11.2.5 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je iznošenje opreme, informacija ili softvera izvan organizacije ograničeno i regulirano prethodnim odobrenjem?										
A.11.2.6 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se zahtjevi vezani uz sigurnost primjenjuju i na imovinu koja se nalazi izvan organizacije uzimajući u obzir različite rizike pri radu izvan prostorija organizacije?										

A.11.2.7 ISMS / 6.8.2.7 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li postoji verifikacija svih dijelova opreme koja sadrži medije za pohranu kako bi se osiguralo da su bilo koji osjetljivi podatci i licencirani softver uklonjeni ili sigurno prebrisani prije odbacivanja opreme ili njenog ponovnog korištenja?										
Postoje li tehničke mjere koje osiguravaju da se pri brisanju osobnih podataka kod preraspodjele prostora za pohranu, uklanjanja medija ili njihove ponovne upotrebe, do njih više ne može doći na niti jedan način?										
U slučaju čuvanja osobnih podataka u informacijskom sustavu i mogućih problema s funkcioniranjem u slučaju izričitog brisanja osobnih podataka, da li su uvedene posebne tehničke mjere kojima će se izbjeći rizik da drugi korisnik može pristupiti osobnim podatcima u sustavu?										
Da li se kod sigurnosnog uklanjanja ili ponovne upotrebe oprema koja sadrži medij za pohranu, a koja potencijalno sadrži osobne podatke tretira na način kao da ih zaista sadrži?										
A.11.2.8 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li je organizacija, i na koji način, osigurala da oprema bez nadzora posjeduje prikladnu zaštitu?										
A.11.2.9 ISMS / 6.8.2.9 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su usvojene politike čistog stola za papire i uklonjive medije te čistog zaslona za opremu za obradu informacija?										
Da li organizacija ograničava stvaranje tiskanog materijala koji uključuje osobne podatke na najmanju moguću mjeru potrebnu za ispunjenje svrhe te obrade podataka?										
A.12 ISMS										
A.12.1 ISMS										
A.12.1.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su radne procedure dokumentirane i dostupne svim korisnicima kojima su potrebne?										

A.12.1.2 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li se nadziru sve promjene u organizaciji, poslovnim procesima, opremi i sustavima za obradu informacija koje imaju utjecaj na informacijsku sigurnost?										
A.12.1.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je nadzirano korištenje resursa i prilagođeno potrebama te da li su napravljene projekcije budućih zahtjeva za kapacitetom kako bi se osigurale zahtijevane performanse sustava?										
A.12.1.4 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su razvojne, testne i operativne okoline odvojene u svrhu smanjenja rizika od neovlaštenog pristupa ili uslijed promjena operativne okoline?										
A.12.2 ISMS										

A.12.2.1 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li su uvedene kontrole za otkrivanje, sprječavanje i oporavak od zlоćudnog softvera u kombinaciji s osiguravanjem primjerene svijesti korisnika o nužnosti provedbe tih kontrola i posljedica rizika uslijed njihovog neprovođenja?										
A.12.3. ISMS										
A.12.3.1 ISMS / 6.9.3.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se sigurnosne kopije (back-up) informacija, softver i serijalizirane kopije stanja računalnog sustava pohranjuju i testiraju u skladu s prihvaćenom politikom vezanom uz izradu sigurnosnih kopija?										
Da li organizacija ima zasebnu politiku ili informacije uključene u politiku oporavka sustava sa sadržajem koji opisuje zahtjeve za sigurnosnu kopiju, oporavak i vraćanje osobnih podataka, kao i sve daljnje zahtjeve za brisanjem osobnih podataka; primjerice ugovornim i/ili pravnim uvjetima?										

Da li je organizacija osigurala da je klijent obaviješten o ograničenjima usluge kad je riječ o sigurnosnoj kopiji ili uslugama oporavka podataka te svim mogućnostima koje klijentu može pružiti u slučaju sigurnosnog kopiranja i oporavka osobnih podataka?											
Da li je organizacija identificirala sve zahtjeve zakonodavstva unutar kojeg djeluje, vezane uz učestalost sigurnosnih kopija osobnih podataka, učestalost pregleda testova sigurnosnih kopija ili procedura oporavka u slučaju osobnih podataka?											
U slučajevima kad su osobni podatci vraćeni sa sigurnosne kopije, da li je organizacija uspostavila procese kako bi osigurala da se osobni podatci nedvojbeno vrate u stanje u kojem može jamčiti njihovu cjelovitost?											
Postoje li procesi u slučaju identifikacije netočnosti i/ili nepotpunosti podataka koji će omogućiti njihov ispravak ili nadopunu, a koji mogu uključivati i aktivnosti vezane uz same ispitanike?											
Posjeduje li organizacija proceduru za evidentiranje postupaka i pokušaja vraćanja osobnih podataka, a koja minimalno sadrži informacije o imenu osobe odgovorne za njihovo vraćanje te opis vraćenih osobnih podataka?											

U slučaju da zakonodavni okvir u kojem organizacija djeluje propisuje sadržaj takvih evidencija, da li je organizacija u mogućnosti dokumentirati sukladnost sa svim primjenjivim zahtjevima vezanim uz vraćanje osobnih podataka te da li su zaključci vezani uz takva razmatranja uključeni u dokumentirane informacije u slučaju neprimjenjivih zahtjeva?										
A.12.4 ISMS										
A.12.4.1 ISMS / 6.9.4.1 PIMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su logovi događaja koji bilježe korisničke aktivnosti, iznimke, pogreške i događaje informacijske sigurnosti kreirani, čuvani i redovito pregledavani?										
Da li je organizacija implementirala proces za pregled evidencija primjenjujući kontinuirane, automatizirane procese za nadzor i upozoravanje, ili druge manualne procese kada je njihov pregled neophodno obavljati prema definiranom i dokumentiranom vremenskom razmaku, a kako bi se prepoznale nepravilnosti i predložile korektivne radnje?										

	Ukoliko organizacija ima tehničku mogućnost, da li logovi događaja stvaraju i dokaze vezane uz identifikaciju osoba koja je pristupila osobnim podatcima, kad, kojim osobnim podatcima je pristupljeno i, ako su učinjene, koje su bile promjene ili rezultati takvih događanja?										
	U slučaju da je u pružanje same usluge uključeno više pružatelja, da li su jasno definirane i dokumentirane njihove uloge te da li su sa svakim od njih ugovorno definirani uvjeti pristupa evidenciji logova?										
	Kad je organizacija u svojstvu izvršitelja obrade, da li je definirala kriterije vezane za to kada i kako evidentirane informacije mogu postati dostupne klijentima te kad ih on smije koristiti?										
	Da li su ti kriteriji dostupni klijentu?										
	Kad je organizacija u svojstvu izvršitelja obrade, da li je uspostavila tehničke mjere u slučajevima da svojim klijentima dozvoljava pristup evidenciji logiranja koju kontrolira organizacija kako bi osigurala da klijent može pristupiti samo evidencijama logova koje se odnose samo na njegovu aktivnost te ne može pristupiti onima koje se odnose na aktivnost drugih klijenata?										
	Kad je organizacija u svojstvu izvršitelja obrade, da li uspostavljene tehničke mjere u slučajevima dozvole pristupa evidenciji logiranja od strane klijenata uključuju i one koje će klijenta onemogućiti da na bilo koji način										

može promijeniti podatke u evidenciji logiranja?										
U slučaju da organizacija koristi videonadzor, da li je uspostavljen automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora koji sadržava vrijeme i mjesto pristupa, kao i oznaku osoba koje su izvršile pristup podatcima prikupljenim putem videonadzora, a u skladu s nacionalnim provedbenim zakonom?										
A.12.4.2 ISMS / 6.9.4.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija zaštitila opremu za kreiranje logova i informacije o logiranju od neovlaštenih izmjena i neovlaštenog pristupa?										
Da li su uspostavljene tehničke mjere poput kontrole pristupa kako bi se osiguralo da se informacije o logiranju koriste samo kako je namjeravano?										
Da li organizacija posjeduje automatsku ili manualnu proceduru kako bi osigurala da informacije o logiranju ne budu izbrisane ili de-identificirane, a sukladno definiranom u planu čuvanja takvih podataka?										

A.12.4.3 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li se bilježe logovi aktivnosti administratora i operatera sustava te da li su zaštićeni i redovito se pregledavaju?										
A.12.4.4 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su satovi svih relevantnih sustava za obradu informacija unutar organizacijske ili sigurnosne domene sinkronizirani prema jedinstvenom referentnom izvoru vremena?										
A.12.5 ISMS										
A.12.5.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se primjenjuju procedure za kontrolu instaliranja softvera na operativne sustave?										
A.12.6. ISMS										

A.12.6.1 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li organizacija pravovremeno prikuplja informacije o tehničkim ranjivostima korištenog sustava, procjenjuje svoju izloženost takvim ranjivostima i poduzima prikladne mjere za obradu pripadajućeg rizika?										
A.12.6.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su uspostavljena i primijenjena pravila koja upravljaju instalacijom softvera od strane korisnika?										
A.12.7 ISMS										
A.12.7.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su zahtjevi i aktivnosti audita odnosno revizije koji uključuju verifikacije operativnih sustava pažljivo planirani i prihvaćeni kako bi se smanjili prekidi poslovnih procesa?										

A.13 ISMS										
A.13.1 ISMS										
A.13.1.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se mreže nadziru i njima se upravlja na način koji će zaštititi informacije u sustavima i aplikacijama?										
A.13.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su sigurnosni mehanizmi, razine usluga i upravljački zahtjevi svih mrežnih usluga identificirani i uključeni u sporazume o mrežnim uslugama, bilo da usluge pruža organizacija ili podizvođač?										
A.13.1.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su grupe informacijskih usluga, korisnika i informacijskih sustava odvojene u mrežama?										

A.13.2 ISMS										
A.13.2.1 ISMS / 6.10.2.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su uvedene formalne politike prijenosa, procedure i kontrole kako bi se zaštitio prijenos informacija putem bilo koje vrste komunikacijske opreme?										
Da li je organizacija razmotrila procedure kako bi osigurala da se pravila koja se odnose na obradu osobnih podataka provode u cijelom sustavu i izvan njega, tamo gdje je to primjenjivo?										
Da li je organizacija prilikom definiranja politika i procedura za prijenos informacija koje sadrže osobne podatke uzela u obzir i moguća ograničenja prilikom prijenosa osobnih podataka s obzirom na njihovu vrstu, način i krajnju lokaciju prijenosa?										
A.13.2.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li sklopljeni sporazumi uključuju siguran prijenos poslovnih informacija između organizacije i vanjskih strana?										

A.13.2.3 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li su informacije uključene u elektroničku razmjenu poruka prikladno zaštićene?										
A.13.2.4 ISMS / 6.10.2.4 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija dokumentirala sve zahtjeve koji odražavaju organizacijske potrebe za zaštitom informacija, a koji se odnose na ugovore o povjerljivosti ili neotkrivanju, te su oni redovito pregledavani i dokumentirani?										
Da li je organizacija osigurala da su i pojedinci koji imaju pristup osobnim podatcima podložni obvezi povjerljivosti putem sporazuma o povjerljivosti ili aneksima ugovora u kojima je točno definirano vrijeme obveze povjerljivosti podataka?										
Kada je organizacija izvršitelj obrade, da li sporazum o povjerljivosti u bilo kojem obliku osigurava da se njeni zaposlenici i agenti moraju pridržavati politika i procedura vezanih uz rukovanje i zaštitu podataka?										
A.14. ISMS										
A.14.1 ISMS										

A.14.1.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su zahtjevi koji se odnose na informacijsku sigurnost uključeni u zahtjeve za nove informacijske sustave ili poboljšanje postojećih informacijskih sustava?										
A.14.1.2 ISMS / 6.11.1.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su informacije uključene u aplikacijske usluge koje prolaze javnim mrežama zaštićene od aktivnosti krivotvorenja, osporavanja ugovora, neovlaštenog otkrivanja i izmjene?										
Da li je organizacija osigurala da se osobni podatci preneseni putem nepouzdanih mreža za prijenos podataka, a koje mogu uključivati javni Internet i druge sadržaje izvan kontrole organizacije, šifrirani?										
A.14.1.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li su informacije uključene u transakcije aplikacijskih usluga zaštićene kako bi se spriječio necjeloviti prijenos, pogrešno usmjeravanje, neovlaštena izmjena poruka, neovlašteno otkrivanje, neovlašteno dupliciranje ili reprodukcija poruka?										
A.14.2 ISMS										
A.14.2.1 ISMS / 6.11.2.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su pravila za razvoj softvera i sustava uspostavljena i primijenjena na razvoj unutar organizacije?										
Da li politike za razvoj i dizajn sustava uključuju i smjernice za organizaciju i njezine potrebe obrade osobnih podataka temeljene na obvezama prema ispitanicima i/ili svakoj primjenjivoj legislativi i/ili regulativi i vrstama obrade koje provodi organizacija?										
Da li politike koje doprinose integriranoj i predefiniranoj privatnosti u obzir uzimaju i smjernice o zaštiti osobnih podataka i implementaciji principa privatnosti unutar životnog ciklusa razvoja softvera?										
Da li se zahtjevi za privatnost i zaštitu osobnih podataka u fazi dizajna temelje na povratnoj informaciji provjera vezanih uz rizike po privatnost i/ili procjene utjecaja na privatnost?										

Postoje li i na koji način su u politikama definirane kontrolne točke vezane uz obrade osobnih podatkaka prilikom važnih prekretnica na projektu?										
Da li je organizacija pri definiranju politika uzela u obzir sve zahtjeve vezane uz privatnost te u svim fazama životnog ciklusa razvoja softvera i sustava obradu osobnih podataka definira u minimalnom opsegu koji omogućava ispunjenje zadane svrhe?										
A.14.2.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su promjene u sustavima unutar razvojnog ciklusa kontrolirane korištenjem formalnih procedura za kontrolu promjene?										
A.14.2.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su kod promjene operativne platforme poslovno kritične aplikacije pregledane i testirane kako bi se osiguralo da ne postoje nepovoljni utjecaji na poslovanje organizacije ili sigurnost?										

A.14.2.4 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li su promjene softverskih paketa strogo kontrolirane i ograničene samo na nužne promjene?										
A.14.2.5 ISMS / 6.11.2.5 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su principi inženjeringa sigurnih sustava uspostavljeni, dokumentirani, održavani i primijenjeni na svaku implementaciju informacijskog sustava?										
Da li su sustavi i/ili njegovi sastavni dijelovi koji su vezani uz obradu osobnih podataka dizajnirani slijedeći principe integrirane ili predefinirane privatnosti te predviđaju i omogućavaju implementaciju relevantnih kontrola s obzirom na ograničenje obrade samo na identificirane svrhe?										
Da li je sustav dizajniran na način da omogućava zahtjev brisanja nakon isteka definiranog vremena čuvanja osobnih podataka?										

A.14.2.6 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je uspostavljena i primjereno zaštićena okolina sigurnog razvoja za razvoj sustava koji se odnose na cijeli životni ciklus sustava?										
A.14.2.7 ISMS / 6.11.2.7 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija nadgleda i nadzire sve aktivnosti razvoja sustava koje obavljaju podizvođači?										
Da li su svi principi integrirane i predefinirane privatnosti, ako je primjenjivo, primijenjeni na informacijske sustave koji su predmetom vanjske usluge?										
A.14.2.8 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se provodi testiranje sigurnosnih funkcionalnosti tijekom razvoja?										

A.14.2.9 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li su uspostavljeni programi testiranja prihvatljivosti i povezani kriteriji za nove informacijske sustave, nadogradnje i nove verzije?										
A.14.3 ISMS										
A.14.3.1 ISMS / 6.11.3.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su testni podatci pažljivo odabrani, zaštićeni i kontrolirani?										
Da li se u najvećoj mogućoj mjeri izbjegava korištenje osobnih podataka te se umjesto njih koriste lažni ili sintetički jednakovrijedni podatci?										
U slučajevima kad se ne može izbjeći korištenje osobnih podataka, da li su u svrhu smanjivanja rizika implementirane tehničke i organizacijske mjere istovjetne onima korištenima u razvojnom okruženju?										
Ukoliko takve mjere nisu primjenjive, da li je provedena procjena rizika i predložena prikladna kontrola za izbjegavanje ili ublažavanje rizika?										

A.15 ISMS										
A.15.1 ISMS										
A.15.1.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su s dobavljačima dogovoreni i dokumentirani svi zahtjevi informacijske sigurnosti za ublažavanje rizika povezanog s njihovim pristupom imovini organizacije?										
A.15.1.2 ISMS / 6.12.1.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija utvrdila i dogovorila sve relevantne zahtjeve informacijske sigurnosti sa svakim dobavljačem koji može pristupiti, obraditi, pohraniti, komunicirati ili pružiti komponente IT infrastrukture za organizacijske informacije?										
Da li su u ugovorima s dobavljačima koji imaju doticaj s osobnim podatcima definirane minimalne tehničke i organizacijske mjere koje moraju ispuniti kako bi organizacija ispunila svoje obveze vezane uz informacijsku sigurnost i zaštitu osobnih podataka?										

Da li su u sporazumima s dobavljačima jasno definirane odgovornosti organizacije, njezinih partnera, dobavljača i primjenjivih trećih strana uzimajući u obzir vrstu osobnih podataka koji se obrađuju?										
Da li sporazumi između organizacije i njezinih dobavljača pružaju mehanizam koji osigurava da organizacija podržava i održava usklađenost s primjenjivim zakonodavstvom i/ili odredbama, a uključuju zahtjeve dokazivanja usklađenosti auditiranjem odnosno revizijom od strane neovisnih izvora?										
Da li definirane tehnike auditiranja odnosno revizije uključuju usklađenost s relevantnim i primjenjivim standardima sigurnosti i privatnosti poput ISO/IEC 27001 i ISO/IEC 27701?										
U slučajevima kad su dobavljači u svojstvu izvršitelja obrade, da li je organizacija u sporazumima s njima specificirala da se osobni podatci obrađuju samo na njen naputak?										
A.15.1.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li sporazumi s dobavljačima uključuju zahtjeve kako bi obradili rizike informacijske sigurnosti i privatnosti povezane s dobavljačkim lancem usluga i proizvoda vezanih uz informacijsko-komunikacijske tehnologije?										

A.15.2 ISMS										
A.15.2.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija redovito nadzire, pregledava i provodi audite odnosno revizije nad isporukama usluga dobavljača?										
A.15.2.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se promjenama u uvjetima pružanja usluga dobavljača, uključujući održavanje i poboljšavanje postojećih politika informacijske sigurnosti, procedura i kontrola, upravlja uzimajući u obzir kritičnost obuhvaćenih poslovnih informacija, sustava i procesa te se provode ponovne procjene rizika?										
A.16. ISMS										
A.16.1 ISMS										
A.16.1.1 ISMS / 6.13.1.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li je organizacija uspostavila upravljačke odgovornosti i procedure kako bi se osigurao brz, djelotvoran i uredan odgovor na incidente informacijske sigurnosti?										
Da li je organizacija uspostavila odgovornosti i procedure vezane uz identifikaciju i evidentiranje povreda nad osobnim podatcima, te obavještavanje odgovarajućih strana o takvim povredama uzimajući u obzir primjenjivo zakonodavstvo i/ili odredbe?										
A.16.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se događaji informacijske sigurnosti prijavljuju putem odgovarajućih kanala i u najkraćem mogućem roku?										
A.16.1.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je od zaposlenika i ugovornih strana koji koriste informacijske sustave i usluge organizacije zahtijevano da zabilježe i izvijeste o bilo kojoj uočenoj sigurnosnoj slabosti ili sumnji na sigurnosnu slabost u sustavima ili uslugama?										

A.16.1.4 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li se događajima informacijske sigurnosti procjenjuje učinak i postoji li procedura odlučivanja o njihovoj klasifikaciji kao incidentima informacijske sigurnosti?										
A.16.1.5 ISMS / 6.13.1.5 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija na incidente informacijske sigurnosti odgovara u skladu s dokumentiranom procedurom?										
Da li organizacija, kod incidenata informacijske sigurnosti koji uključuju osobne podatke, unutar procesa upravljanja incidentima utvrđuje i da li su mogli dovesti do povrede osobnih podataka te, ukoliko jesu, na koji način se o njima očituje?										
Kod povreda nad osobnim podatcima, da li procedure odgovora na incidente uključuju i relevantne obavijesti i evidencije?										
Da li su definirani kriteriji za obavještavanje nadzornog tijela i ispitanika u slučajevima povreda nad osobnim podatcima, za voditelja i izvršitelja obrade?										

Da li su obavijesti jasne i sadržavaju i detalje poput kontakta i mjesta za dobivanje više informacija, opisa i moguće posljedice povrede, opisa povrede s brojem uključenih osoba i kompromitiranih evidencija te poduzete mjere ili mjera koje se tek planiraju poduzeti?											
Da li evidencija o povredama nad osobnim podatcima sadržava nužne podatke za kreiranje izvještaja, a koji sadržavaju opis incidenta, vremensko razdoblje nastanka povrede, posljedice incidenta, ime osobe koja je izvijestila o povredi, adresate priopćenja o povredi, poduzete korake u rješavanju incidenta koji uključuju ime nadležne osobe i vraćene podatke te opisu činjeničnog stanja o nastanku i rezultatima incidenta (nedostupnost, gubitak, otkrivanje ili izmjene osobnih podataka)?											
U slučaju kad je organizacija izvršitelj obrade, da li su odredbe koje pokrivaju obavijesti o povredi nad osobnim podatcima obuhvaćene sporazumima između organizacije i klijenta?											
Da li je u tom sporazumu definiran i način na koji organizacija pruža informacije klijentu da ispuni svoju obvezu obavještavanja relevantnih nadležnih tijela, a koja ne obuhvaća povredu koju je učinio klijent ili ispitanik ili koja je unutar sistemskih komponenti za koje su oni odgovorni?											
Na koji način je organizacija odredila obavještavanje voditelja obrade u slučaju da je ona kao izvršitelj obrade uočila povredu nad osobnim podatcima?											

Da li organizacija, i u slučaju kad je izvršitelj obrade, vodi evidencije o povredama nad osobnim podatcima, a koje uključuju sve gore navedene podatke nužne za kreiranje izvještaja?										
A.16.1.6 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se znanje prikupljeno analizom i rješavanjem incidenata informacijske sigurnosti koristi za smanjenje vjerojatnosti ili utjecaja budućih incidenata?										
A.16.1.7 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija definirala i primijenila procedure za identifikaciju, prikupljanje, pribavljanje i očuvanje informacija koje mogu poslužiti kao dokaz?										
A.17 ISMS										
A.17.1 ISMS										

A.17.1.1 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija odredila svoje zahtjeve za informacijsku sigurnost i za neprekinutost upravljanja informacijskom sigurnosti u nepovoljnim situacijama poput krize ili katastrofa?										
A.17.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija utvrdila, dokumentirala, primijenila i održava procese, procedure i kontrole kako bi osigurala zahtijevanu razinu neprekinutosti informacijske sigurnosti tijekom nepovoljne situacije?										
A.17.1.3 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija redovito verificira uspostavljene i primijenjene kontrole neprekinutosti informacijske sigurnosti kako bi osigurala njihovu valjanost i djelotvornost za vrijeme nepovoljnih situacija?										

A.17.2. ISMS										
A.17.2.1 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je oprema za obradu informacija implementirana s redundancijom dostatnom kako bi ispunila sve zahtjeve vezane uz raspoloživost?										
A.18. ISMS										
A.18.1 ISMS										
A.18.1.1 ISMS / 6.15.1.1 PIMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija definirala, dokumentirala i drži ažuriranima sve relevantne zakonske, statutarne, regulatorne i ugovorne zahtjeve za svaki informacijski sustav?										
Da li je organizacija identificirala i sve potencijalne sankcije koje mogu uslijediti propuštanjem propisane ili preuzete obveze vezane uz obradu osobnih podataka?										

Da li je organizacija uzela u obzir i nacionalni provedbeni zakon te njegove odredbe u postupcima u nadležnosti nadzornog tijela, vezane uz povredu prava po osobnim podatcima?										
A.18.1.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su primijenjene odgovarajuće procedure kako bi se osigurala sukladnost sa zakonskim, regulatornim i ugovornim zahtjevima povezanim s pravima intelektualnog vlasništva i s korištenjem vlastitih softverskih proizvoda?										
A.18.1.3 ISMS / 6.5.1.3 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su zapisi zaštićeni od gubitka, uništenja, krivotvorenja, neovlaštenog pristupa i neovlaštenog objavljivanja, te u skladu sa zakonskim, regulatornim, ugovornim i poslovnim zahtjevima?										
Da li organizacija zadržava kopije svojih aktualnih verzija politika privatnosti i vezanih procedura, kao i njihovih prethodnih verzija s datumima ažuriranja, u razdoblju definiranom planom čuvanja podataka?										

A.18.1.4 ISMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je osigurana privatnost i zaštita osobnih podataka kako je zahtijevano u relevantnoj legislativi i regulativi, gdje je primjenjivo?										
A.18.1.5 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li su kriptografske kontrole korištene u skladu sa svim relevantnim sporazumima, zakonima i regulativom?										
A.18.2 ISMS										
A.18.2.1 ISMS / 16.5.2.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija provodi neovisan pregled cjelokupnog sustava upravljanja informacijskom sigurnosti u planiranim intervalima ili po događanju značajnih promjena?										

Kad je organizacija izvršitelj obrade, može li klijentima omogućiti, prije sklapanja i za vrijeme trajanja ugovorne obveze, dokaz rezultata nezavisnog audita odnosno revizije sustava kojim je vidljivo da je informacijska sigurnost implementirana te da funkcionira sukladno definiranim politikama i procedurama organizacije?										
A.18.2.2 ISMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li menadžeri redovito pregledavaju sukladnost obrade informacija i procedura unutar njihova područja odgovornosti s primjerenim informacijskim politikama, standardima i bilo kojim sigurnosnim zahtjevima?										
A.18.2.3 ISMS / 16.5.2.3 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li se informacijski sustavi redovito pregledavaju kako bi se utvrdila usklađenost s politikama i standardima informacijske sigurnosti organizacije?										

Da li je organizacija u tehničke preglede usklađenosti sa sigurnosnim politikama i standardima uključila i metode pregleda alata i komponenata povezanih s obradom osobnih podataka, a koji uključuju kontinuirani nadzor u svojstvu potvrde da se provodi samo dozvoljena obrada i/ili penetracijske testove kako bi validirala da su metode de-identifikacije osobnih podataka sukladne organizacijskim zahtjevima?										

Procjena usklađenosti organizacijskih i tehničkih mjera sa specifičnim PIMS ciljevima i kontrolama ISO/IEC 27701 u skladu s ISO 19011 i nacionalnim provedbenim zakonom										
VODITELJI OBRADE, Aneks A										
A.7.2 PIMS										
A.7.2.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija identificirala i dokumentirala posebne svrhe u koje će se obrađivati osobne podatke?										

A.7.2.2 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija utvrdila, dokumentirala i pridržava se relevantne zakonske osnove za obradu osobnih podataka u identificirane svrhe?										
A.7.2.3 PIMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija utvrdila i evidentirala proces kojim u svakom trenutku može demonstrirati kada i na koji način je dobila privolu ispitanika za obradu osobnih podataka?										
Da li je organizacija utvrdila uvjete i zahtjeve propisane, uz ostalo, i nacionalnim provedbenim zakonom, a koje se odnose na dobivanje privole u posebnim slučajevima?										
A.7.2.4 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija dobila i evidentirala privolu ispitanika za obradu osobnih podataka u skladu s dokumentiranim procesima?										

A.7.2.5 PIMS / NPZ	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija, prilikom planiranja nove obrade ili promjene nad postojećim obradama osobnih podataka implementirala proces izvedbe i po potrebi izvodi procjene utjecaja na privatnost?										
Da li je organizacija, u slučaju korištenja sustava biometrijske obrade podataka, napravila procjenu njegovog učinka na privatnost sukladno nacionalnom provedbenom zakonu?										
A.7.2.6 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija ima pisani sporazum sa svakim izvršiteljem obrade kojeg koristi, a koji uključuje implementaciju odgovarajućih kontrola koji se tiču odnosa s izvršiteljima obrada?										
A.7.2.7 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li organizacija može odrediti pojedinačne uloge i odgovornosti za obradu osobnih podataka sa svakim zajedničkim voditeljem obrade uključujući aspekte njihove zaštite i sigurnosnih zahtjeva?										
A.7.2.8 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija utvrdila i na siguran način održava sve potrebne evidencije kojima dokazuje svoje obveze prema obradi osobnih podataka?										
A.7.3 PIMS										
A.7.3.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija utvrdila i evidentirala sve pravne, regulatorne i poslovne obveze prema ispitanicima čije osobne podatke obrađuje te omogućila transparentan način dokazivanja ispunjenja tih obveza?										

A.7.3.2 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija utvrdila i evidentirala informacije koje će na njihov zahtjev pružiti ispitanicima čije osobne podatke obrađuje, kao i definirala vremenski okvir u kojem će taj zahtjev izvršiti?										
A.7.3.3 PIMS / NPZ	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija ispitanicima čije osobne podatke obrađuje pruža jasne i lagano dostupne informacije u kojima je nedvojbeno naveden voditelj obrade te opisana obrada njihovih osobnih podataka?										
Da li je organizacija pri definiranju opsega informacija koje pruža ispitanicima uzela u obzir i zahtjeve propisane nacionalnim provedbenim zakonom?										
A.7.3.4 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija omogućava mehanizam kojim ispitanici čiji se osobni podatci obrađuju mogu izmijeniti ili povući svoju privolu?										

A.7.3.5 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija ispitanicima čije osobne podatke obrađuje pruža mehanizam za ulaganje prigovora na obradu njihovih podataka?										
A.7.3.6 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija implementirala politike, procedure i/ili mehanizme kako bi ispitanicima čije osobne podatke obrađuje omogućila pristup tim podatcima, ispravak i/ili njihovo brisanje?										
A.7.3.7 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija implementirala odgovarajuće politike, procedure i/ili mehanizme kojima može obavijestiti treće strane s kojima dijeli osobne podatke o svim izmjenama, povlačenjima privola ili prigovorima vezanim uz njihovo dijeljenje?										

A.7.3.8 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija u mogućnosti ispitanicima čije osobne podatke obrađuje predati kopiju osobnih podataka pojedinog ispitanika na njegov osobni zahtjev?										
A.7.3.9 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija definirala i evidentirala sve politike i procedure za postupanje i odgovaranje na legitimne zahtjeve ispitanika čije osobne podatke obrađuje?										
A.7.3.10 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija identificirala i navela sve obveze prema ispitanicima čije osobne podatke obrađuje, uključujući i pravne, a koje su rezultat odluka organizacije i tiču se automatizirane obrade njihovih podataka?										
A.7.4 PIMS										

A.7.4.1 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija ograničila prikupljanje osobnih podataka na najmanju moguću mjeru koja je relevantna, proporcionalna i nužna za ispunjenje identificirane svrhe?										
A.7.4.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija ograničila obradu osobnih podataka samo na prikladno, relevantno i nužno za identificirane svrhe?										
A.7.4.3 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija osigurala i dokumentirala ispunjenje uvjeta da su osobni podatci koje obrađuje što točniji, potpuniji i ažurni tijekom cijelog svog životnog vijeka obrade do ispunjenja svrhe?										

A.7.4.4 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija definirala i evidentirala ciljeve za minimalizaciju osobnih podataka te mehanizme koje koristi za de-identifikaciju u ispunjenju tih ciljeva?										
A.7.4.5 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija, nakon što originalni osobni podatci više nisu potrebni u svrhu identifikacije, briše ili ne dopušta daljnju ili ponovnu identifikaciju tog ispitanika?										
A.7.4.6 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija osigurala da se i privremene datoteke nastale kao rezultati obrade osobnih podataka izbrišu ili unište prema dokumentiranim postupcima u za to određenom roku?										

A.7.4.7 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li organizacija čuva osobne podatke i duže nego što je potrebno za ispunjenje svrha u koje su bili obrađivani?										
A.7.4.8 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija ima dokumentirane politike, procedure i/ili mehanizme za uklanjanje osobnih podataka?										
A.7.4.9 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija kod slanja osobnih podataka putem mreže za prijenos podataka primjenjuje odgovarajuće kontrole kako bi osigurala da ti podatci sigurno stignu na njihovu namjeravanu destinaciju?										
A.7.5 PIMS										

A.7.5.1 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija identificirala i dokumentirala relevantnu osnovu za prijenos osobnih podataka između nadležnosti?										
A.7.5.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija definirala i dokumentirala zemlje i međunarodne organizacije kojima se potencijalno mogu prenijeti osobni podaci?										
A.7.5.3 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija evidentirala prijenose osobno identificirajućih podataka prema ili od trećih strana te osigurala potpunu suradnju s tim stranama u svrhu podrške budućim zahtjevima vezanim uz obveze prema ispitanicima čije osobne podatke obrađuje?										

A.7.5.4 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li organizacija evidentira ili ima ustanovljen proces evidentiranja otkrivanja osobnih podataka trećim stranama, uključujući informacije o tome koji su podatci otkriveni, kome i kada?										
Procjena usklađenosti organizacijskih i tehničkih mjera sa specifičnim PIMS ciljevima i kontrolama ISO/IEC 27701 u skladu s ISO 19011										
IZVRŠITELJI OBRADE, Aneks B										
B.8.2 PIMS										
B.8.2.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija osigurala da, u slučajevima kad je to potrebno, ugovori vezani uz obradu osobnih podataka uključuju i ulogu same organizacije u pružanju pomoći s klijentovim obvezama s obzirom na prirodu obrade i informacije dostupne organizaciji?										

B.8.2.2 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li je organizacija osigurala da su osobni podatci obrađeni u ime klijenta obrađeni samo u svrhe koje su navedene u evidentiranim uputama od klijenta?										
B.8.2.3 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija koristi osobne podatke prema ugovoru u marketinške ili oglašivačke svrhe bez prethodne potvrde da je za to dobivena privola ispitanika čiji osobni podaci se obrađuju te da li je privola dobivena ikakvim uvjetovanjem primanja usluge?										
B.8.2.4 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li će organizacija obavijestiti klijenta ukoliko ustanovi da uputa za obradu osobnih podataka krši primjenjivu legislativu i/ili regulativu?										

B.8.2.5 PIMS	C	NC MJ	NC MI	PI	N/A	obrazloženje N/A	obrazloženje PI	audit dokaz	korektivna radnja u slučaju NC MJ i NC MI	rok rješavanja u slučaju NC MJ i NC MI
Da li organizacija klijentu pruža odgovarajuće informacije na način da njima klijent može iskazati sukladnost sa svojim obvezama?										
B.8.2.6 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija utvrdila i održava potrebne evidencije kako bi pokazala usklađenost sa svojim obvezama definiranima primjenjivim sporazumima, za obrade osobnih podataka izvršene u klijentovo ime?										
B.8.3 PIMS										
B.8.3.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Može li organizacija pružiti klijentu sredstva da zadovolji usklađenost sa svojim obvezama vezanim uz ispitanike čije osobne podatke obrađuje?										

B.8.4 PIMS										
B.8.4.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija osigurala da se privremene datoteke kreirane kao rezultat obrade osobnih podataka mogu ukloniti brisanjem ili uništavanjem slijedeći dokumentirane postupke unutar dokumentiranog određenog roka?										
B.8.4.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Može li organizacija pružiti mogućnost povrata, prijenosa i/ili uklanjanja osobnih podataka na siguran način te da li je njena politika vezana uz te informacije dostupna klijentu?										
B.8.4.3 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija podvrgava osobne podatke poslane putem mreže za prijenos podataka odgovarajućim kontrolama dizajniranim da osiguraju dostavu podataka na njihovu namjeravanu destinaciju?										

B.8.5 PIMS										
B.8.5.1 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija može pravovremeno obavijestiti klijenta o osnovi za prijenos osobnih podataka među nadležnostima i o svim namjeravanim promjenama u tom smislu, tako da klijent ima mogućnost prigovoriti na takve promjene ili raskinuti ugovor?										
B.8.5.2 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li je organizacija definirala i dokumentirala zemlje i međunarodne organizacije kojima se osobni podatci potencijalno mogu prenijeti?										
B.8.5.3 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li organizacija evidentira ili ima ustanovljen proces evidentiranja otkrivanja osobnih podataka trećim stranama, uključujući informacije o tome koji su podatci otkriveni, kome i kada?										
B.8.5.4 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija obavještava klijenta o svakom zakonski obvezujućem zahtjevu za otkrivanjem osobnih podataka?										
B.8.5.5 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija odbacuje sve zahtjeve za otkrivanjem Posobnih podataka koji nisu zakonski obvezujući, savjetujući se s klijentom prije takvog otkrivanja i prihvaćanja svakog sporazumno dogovorenog zahtjeva za otkrivanjem koji je odgovarajući klijent odobrio?										
B.8.5.6 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**

Da li organizacija otkriva klijentu točan naziv podugovoritelja usluge prije njegovog angažmana vezanog uz obradu osobnih podataka?										
B.8.5.7 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija angažira podugovoritelje za obrade vezane uz osobne podatke samo u skladu sa sporazumom koji ima s klijentom?										
B.8.5.8 PIMS	**C**	**NC MJ**	**NC MI**	**PI**	**N/A**	**obrazloženje N/A**	**obrazloženje PI**	**audit dokaz**	**korektivna radnja u slučaju NC MJ i NC MI**	**rok rješavanja u slučaju NC MJ i NC MI**
Da li organizacija, u slučaju da posjeduje opće pisano odobrenje odnosno obavještava klijenta o svakoj namjeravanoj promjeni vezanoj uz dodavanje ili zamjenu podugovoritelja obrade osobnih podataka te mu omogućava prigovor na takvu promjenu?										

6. Prikaz i analiza rezultata istraživanja

6.1. Metodologija i uzorak

Poziv na sudjelovanje u istraživanju objavljen je na naslovnici poslovnog portala Lider te putem kanala društvenih mreža Facebook, Instagram i LinkedIn.

Uzorak je prigodan, a sudjelovanje je bilo dragovoljno. Potencijalni sudionici dobili su poveznicu na kojoj se nalazio anketni upitnik, s objašnjenjem projekta i zamolbom za sudjelovanje u znanstvenom istraživanju vezanom uz doktorsku disertaciju „Model upravljanja informacijskom sigurnošću u usklađivanju s europskom pravnom regulativom zaštite podataka“.

Prikupljanje podataka provedeno je u razdoblju od 11. do 25. ožujka 2020. godine. Ispunjavanje upitnika u prosjeku je trajalo 5 minuta i 55 sekundi.

U istraživanju su sudjelovala ukupno 142 ispitanika, a nakon što je troje ispitanika diskvalificirano prema kriterijima poznavanja termina „Opća uredba o zaštiti podataka“ i uključenosti u pitanja o zaštiti osobnih podataka u njihovoj organizaciji, analizirani su podatci ukupno 139 ispitanika

Od ukupnog broja ispitanika, 99 (71,2 %) je zaposleno u organizacijama koje djeluju u privatnom sektoru, a 40 ispitanika (28,8 %) zaposleno je u organizacijama iz javnog sektora. Struktura uzorka prema sektoru prikazana je u Tablici 11.

Najviše je ispitanika zaposleno u mikro i malim organizacijama s manje od 10 zaposlenih, njih 46 ili 33,1 % uzorka; 36 ispitanika (25,9 % uzorka) radi u organizacijama s 10 do 49 zaposlenika, 16 ispitanika (11,5 % uzorka) u organizacijama s 50 do 99 zaposlenih, 15 ispitanika (10,8 % uzorka) u organizacijama sa 100 do 249 zaposlenih, te 26 ispitanika (18,7 % uzorka) u organizacijama s 250 i više zaposlenih. Distribucija odgovora na pitanje o broju zaposlenih u organizaciji nalazi se u Tablici 12.

Tablica 15. Struktura uzorka prema sektoru

		Broj ispitanika	%
Sektor	Privatni sektor	99	71,2
	Javni sektor	40	28,8
Ukupno		139	100,0

Tablica 16. Struktura uzorka prema broju zaposlenih

		Broj ispitanika	%
Broj zaposlenih	0 do 9 zaposlenih	46	33,1
	10 do 49 zaposlenih	36	25,9
	50 do 99 zaposlenih	16	11,5
	100 do 249 zaposlenih	15	10,8
	250 i više zaposlenih	26	18,7
Ukupno		139	100,0

6.2. Statistička analiza podataka

Podatci prikupljeni u *on-line* istraživanju analizirani su sukladno postavljenim pretpostavkama o povezanosti stupnja implementacije usklađenosti s Općom uredbom o zaštiti podataka s izostankom procesno primjenjivog modela usklađivanja organizacija s Uredbom. Također je provjerena povezanost ostalih varijabli, točnije veličine organizacije, kompleksnosti obrade osobnih podataka u organizaciji te postojanja različitih ISO standarda, posebice ISO/IEC 27001, u organizacijama i korištenja konzultantskih usluga u procesu usklađivanja s Uredbom.

Analiza podataka provedena je pomoću IBM SPSS v19 statističkog softvera.

Pregled rezultata analize u nastavku rada prati testiranje postavljenih hipoteza elaboriranih u prethodnim poglavljima. Na kraju analize prikazani su i rezultati ostalih pitanja zanimljivih za razmatranje u kontekstu poslovanja organizacija u privatnom vlasništvu sa zemljama Europske unije.

H1 Izostanak procesno primjenjivog modela usklađivanja organizacija s Općom uredbom o zaštiti podataka povezan je s njihovim otežanim usklađivanjem ili s potpunim izostankom usklađivanja

U sklopu Hipoteze 1 provjeren je odnos percipirane težine usklađivanja s Općom uredbom o zaštiti podataka preko tri pokazatelja koji izravno ukazuju na potrebu za uvođenjem procesno primjenjivog modela koji bi olakšao usklađivanje organizacija s Uredbom.

Pretpostavka je da će se poteškoće u procesu usklađivanja uočavati kod razumijevanja obveza propisanih Uredbom, potrebe za angažmanom vanjskih konzultanata u procesu usklađivanja te stupnjem prilagodbe poslovanja zahtjevima Uredbe. U odnos su stavljeni percipirana težina usklađivanja organizacija i trenutni stupanj usklađenosti poslovanja organizacija s Uredbom, percipirana težina usklađivanja organizacija s Uredbom i razumijevanje novih obveza propisanih Uredbom te percipirana težina usklađivanja organizacija i angažman vanjskih konzultanata tijekom procesa usklađivanja.

Kod testiranja ove hipoteze korišteno je pitanje o percepciji težine usklađivanja koje je glasilo: *Proces uvođenja Opće uredbe o zaštiti podataka u Vašu organizaciju biste opisali kao ….* Za procjenu težine korištena je ljestvica od pet stupnjeva: izuzetno težak, uglavnom težak, osrednje težak, uglavnom lagan i izuzetno lagan.

Na pitanje o percepciji težine usklađivanja odgovarali su ispitanici čije su organizacije u trenutku sudjelovanja u istraživanju uskladile svoje poslovanje s Općom uredbom o zaštiti podataka, zatim oni u čijim je organizacijama taj proces u tijeku, te ispitanici čije organizacije planiraju uskladiti svoje poslovanje s Općom uredbom o zaštiti podataka. Ispitanici koji nisu upoznati s Uredbom i oni čija organizacija nije obveznik usklađivanja s Općom uredbom o

zaštiti podataka nisu sudjelovali u testiranju hipoteze o percepciji težine uvođenja Opće uredbe o zaštiti podataka Prema opisanom kriteriju trenutnog stupnja usklađenosti s Uredbom u analizama koje uključuju pitanje o percepciji težine usklađivanja sudjelovalo je 123 ispitanika. Odgovori na pitanje o težini procesa uvođenja Uredbe prikazani su u Tablici 13.

Tablica 17. Distribucija odgovora na pitanje o percipiranoj težini uvođenja Opće uredbe o zaštiti podataka u organizaciju

		Broj ispitanika	%
Percepcija težine uvođenja Opće uredbe o zaštiti podataka	Izuzetno težak	4	3,3
	Uglavnom težak	20	16,3
	Osrednje težak	63	51,2
	Uglavnom lagan	25	20,3
	Izuzetno lagan	11	8,9
Ukupno		123	100,0
Prosječna vrijednost (aritmetička sredina)		123	3,15
Standardna devijacija		123	0,915

H1.1 Provjera povezanosti percipirane težine uvođenja usklađenosti s Općom uredbom o zaštiti podataka sa stupnjem njegove implementacije

Hipoteza o razlikama u poteškoćama u procesu usklađivanja s Općom uredbom o zaštiti podataka s obzirom na trenutni stupanj usklađenosti provjerena je parametrijskim testiranjem rezultata triju skupina ispitanika. U prvoj su skupini bili ispitanici čija je organizacija u potpunosti uskladila svoje poslovanje s Općom uredbom o zaštiti podataka, u drugoj oni u čijim je organizacijama taj proces u tijeku, a u trećoj ispitanici čije organizacije planiraju usklađivanje s Uredbom.

Prosječne vrijednosti skupina i rezultati testiranja jednosmjernom analizom varijance koja je korištena u ovom slučaju prikazani su u Tablici 14. Prije provođenja analize, Levenovim testom

za testiranje homogenosti varijance potvrđena je nul hipoteza da se razlike između varijanci skupina značajno ne razlikuju (Levene t = 1,369; p = 0,258).

Dobivene razlike u rezultatima na skali percipirane težine usklađivanja s Uredbom između ispitanika s obzirom na trenutni stupanj usklađenosti, statistički su značajne. Hipoteza o utjecaju sadašnjeg stupnja usklađenosti je potvrđena (F = 7,119; p = 0,001).

Tablica 18. Rezultati testiranja razlika u percipiranoj težini usklađivanja s Uredbom s obzirom na stupanj usklađenosti organizacije s Uredbom

Percipirana težina usklađivanja		Broj ispitanika	Aritmetička sredina	Std. devijacija	Std. pogreška	F	Stupnjevi slobode	Značajnost p
Stupanj usklađenosti	Da, u potpunosti smo uskladili	88	3,34	,856	,091	7,119	2; 120	0,001
	Proces usklađivanja je u tijeku	30	2,67	,844	,154			
	Planiramo usklađivanje	5	2,80	1,304	,583			

Kako se jednosmjernom analizom varijance istovremeno testira više skupina, za točan uvid u podatkak o tome koje se skupine međusobno razlikuju bilo je potrebno provesti dodatno, tzv. post hoc testiranje parova skupina ispitanika. U tu svrhu korišten je Scheffeov test koji se standardno koristi za testiranje razlika između pojedinih parova skupina ispitanika u slučaju kad F-test kod analize varijance pokaže značajnost razlika. Budući da F-test pokazuje kako postoji statistički značajna razlika među skupinama, ali ne i konkretno između kojih skupina, proveden je i post-hoc test koji ima svrhu utvrđivanja onih parova skupina ispitanika između kojih postoji statistički značajna razlika u ocjenama. Postoji više takvih statističkih testova, ali se najčešće koristi Scheffeov test koji je dosta fleksibilan u terminima zavisnosti o distribuciji rezultata.

Organizacije koje su u potpunosti uskladile poslovanje s Općom uredbom o zaštiti podataka statistički se značajno razlikuju od onih kojima je proces usklađivanja u tijeku (p = 0,002).

Drugim riječima, ispitanici čije su organizacije već provele usklađivanje s Uredbom taj proces procjenjuju lakšima od ispitanika čije su organizacije u procesu usklađivanja poslovanja s Uredbom (prosječna ocjena organizacija koje su u potpunosti uskladile poslovanje je 3,34, a kod organizacija kod kojih je proces u tijeku prosječna ocjena je 2,67; niža ocjena označava veću težinu).

Broj ispitanika zaposlenih u organizacijama koje planiraju uskladiti poslovanje s Općom uredbom o zaštiti podataka je premalen (5), stoga se dobivene razlike u percepciji težine uvođenja Uredbe nisu pokazale statistički značajno različitima od preostale dvije skupina organizacija ($p = 0,405$; $p = 0,951$).

Tablica 19. Rezultati testiranja razlika u ocjenama težine usklađivanja s Uredbom između pojedinačnih parova skupina ispitanika Scheffeovim post-hoc testom

	(I) Jeste li uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?	(J) Jeste li uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?	Razlika prosječnih ocjena (I-J)	Standardna devijacija	Značajnost p
Scheffe test	Da, u potpunosti smo uskladili	Proces usklađivanja je u tijeku	,674	,184	,002
		Planiramo usklađivanje s Općom uredbom o zaštiti podataka	,541	,401	,405
	Proces usklađivanja je u tijeku	Da, u potpunosti smo uskladili	-,674	,184	,002
		Planiramo usklađivanje s Općom uredbom o zaštiti podataka	-,133	,421	,951
	Planiramo usklađivanje s Općom uredbom o zaštiti podataka	Da, u potpunosti smo uskladili	-,541	,401	,405
		Proces usklađivanja je u tijeku	,133	,421	,951

H1.2 Provjera povezanosti percipirane težine uvođenja usklađenosti s Općom uredbom o zaštiti podataka s razumijevanjem novih obveza propisanih u njoj

Hipoteza o povezanosti poteškoća u procesu usklađivanja s Općom uredbom o zaštiti podataka i stupnja razumijevanja novih obveza organizacija propisanih ovom Uredbom provjerena je korelacijskom analizom. U analizi su korištene vrijednosti odgovora na pitanje o razumijevanju novih obveza (prikaz u Tablici 20) i vrijednosti varijable percipirane težine usklađivanja s uredbom.

Većina ispitanika je razumjela obveze organizacija propisane Uredbom, ukupno njih 91,8 %. Obveze je u potpunosti razumjelo 49,2 %, djelomično ih je uz potrebu za dodatnim stručnim pojašnjenjima razumjelo 41,5 %, dok je 9,2 % ispitanika uglavnom nije razumjelo nove obveze organizacija.

Tablica 20. Distribucija odgovora na pitanje o razumijevanju novih obveza organizacija propisanih Općom uredbom o zaštiti podataka

		Broj ispitanika	%
Razumijevanje novih obveza	Uglavnom niste razumjeli	12	9,2
	Dijelom ste razumjeli, ali trebate dodatna pojašnjenja pravnika – stručnjaka za to područje	54	41,5
	Razumjeli ste u potpunosti	64	49,2
Ukupno		130	100,0
Prosječna vrijednost (aritmetička sredina)		130	2,40
Standardna devijacija		130	0,654

Korišten je Pearsonov koeficijent korelacije kojim se provjerava visina i smjer povezanosti između varijabli. Korelacija je mjera povezanosti kojom se mjeri smjer (pozitivna ili negativna povezanost) i visina povezanosti (niska, srednja ili visoka). Pozitivna povezanost znači da je rast/pad jedne vrijednosti prati rast/pad druge, dok je kod negativne povezanosti obrnuto, rast

jedne vrijednosti prati pad druge, odnosno pad jedne praćen je rastom vrijednosti druge varijable. Zbog toga korelacija varira od -1 do +1, a vrijednost 0 je indikator izostanka korelacije. Korelacije manje od 0.30 (bez obzira na predznak) ukazuju na nisku ili nikakvu povezanost rezultata, one u rasponu od 0,30 do 0,70 na srednju povezanost, dok su vrijednosti veće od 0,70 primjer visokog stupnja povezanosti između rezultata dviju varijabli.

Rezultati testiranja korelacijske analize prikazani su u Tablici 21. Dobivena je niska pozitivna povezanost između testiranih varijabli, r = 0.285; p = 0,002. Povezanost je statistički značajna čime je potvrđena postavljena hipoteza. Može se zaključiti da ispitanici koji pokazuju bolje razumijevanje novih obveza propisanih Općom uredbom o zaštiti podataka, procjenjuju proces usklađivanja s odredbama Uredbe lakšim.

Tablica 21. Distribucija odgovora na pitanje o razumijevanju novih obveza organizacija propisanih Općom uredbom o zaštiti podataka

		Proces uvođenja Opće uredbe o zaštiti podataka u Vašu organizaciju biste opisali kao
Jeste li razumjeli nove obveze organizacija propisane Općom uredbom o zaštiti podataka?	Pearson r	,285
	Značajnost p	,002
	Broj ispitanika	120

H1.3 Provjera povezanosti percipirane težine uvođenja usklađenosti s Općom uredbom o zaštiti podataka s korištenjem usluga vanjskih konzultanata pri usklađivanju

Hipoteza o povezanosti poteškoća u procesu usklađivanja s Općom uredbom o zaštiti podataka i načina usklađivanja poslovanja s Općom uredbom o zaštiti podataka provjerena je t-testom za nezavisne uzorke. U analizi su korišteni odgovori na pitanje o načinu usklađivanja poslovanja s Uredbom. Na temelju odgovora na pitanje o načinu usklađivanja ispitanici su podijeljeni u dvije skupine, na one koji su usklađivanje proveli potpuno samostalno i one koji su ga napravili

uz manju ili veću pomoć konzultanata. Oko dvije trećine ispitanika (65,9 %) usklađivanje je obavilo uz pomoć konzultanata, dok je ostatak taj proces obavio potpuno samostalno (podatci su prikazani u Tablici 22.).

Tablica 22. Distribucija odgovora na pitanje o razumijevanju novih obveza organizacija propisanih Općom uredbom o zaštiti podataka

		Broj ispitanika	%
Način usklađivanja poslovanja s Uredbom	Uz manju ili veću pomoć konzultanata	81	65,9
	Potpuno samostalno	42	34,1

Statistička značajnost između prosječenih vrijednosti odgovora na pitanje o težini usklađivanja poslovanja s Općom uredbom o zaštiti podataka između organizacija koje su ovaj proces obavile samostalno i onih koje su to obavile uz pomoć konzultanata testirana je t-testom za nezavisne uzorke. Dobivena razlika između rezultata skupina nije statistički značajna ($t = 0,724$; $p = 0,471$). Prethodno je provjerena homogenost varijance rezultata skupina Levenovim testom koji je pokazao da razlika u varijancama nije statistički značajna (Levene $t = 1,536$; $p = 0,218$).

Rezultati t-testa prikazani u Tablici 23. ukazuju da dobivena razlika u prosječnim vrijednostima percipirane težine uvođenja Uredbe između skupina nije statistički značajna ($t = 0,724$; $p = 0,471$). S obzirom na izostanak potvrde statistički značajne razlike, može se zaključiti da su organizacije koje su proces usklađivanja poslovanja s Uredbom obavile samostalno i one koji su usklađivanje obavile uz stručnu pomoć konzultanata, proces usklađivanja percipiraju jednako zahtjevnim.

Tablica 23. Rezultati testiranja razlika u percipiranoj težini usklađivanja s Uredbom s obzirom na način usklađivanja poslovanja s Općom uredbom o zaštiti podataka

Percipirana težina usklađivanja		Broj ispitanika	Aritmetička sredina	Std. devijacija	Std. pogreška	t	Stupnjevi slobode	Značajnost p
Način usklađivanja poslovanja s Uredbom	Uz manju ili veću pomoć konzultanata	81	3,20	,941	,105	,724	121	,471
	Potpuno samostalno	42	3,07	,867	,134			

Zaključci koji slijede iz testiranja Hipoteze 1:

1. Organizacije koju su u potpunosti dovršile proces usklađivanja s Općom uredbom o zaštiti podataka smatraju taj proces lakšim od onih kod kojih je taj proces još uvijek u tijeku.
2. Ispitanici koji bolje razumiju nove obveze Opće uredbe o zaštiti podataka procjenjuju proces usklađivanja s odredbama Uredbe lakšim.
3. Percepcija težine usklađivanja organizacije s Općom uredbom o zaštiti podataka ne ovisi o tome je li organizacija usklađivanje obavila samostalno ili uz pomoć konzultanata.

H2 ***Korištenje ISO certifikata pri ispunjavanju propisanih zahtjeva za zaštitom osobnih podataka olakšava implementaciju usklađenosti s Općom uredbom o zaštiti podataka***

Poglavlje u kojem su prikazani rezultati testiranja Hipoteze 2 o utjecaju korištenja ISO certifikata na implementaciju usklađenosti s Općom uredbom o zaštiti podataka podijeljeno je na dio u kojem se provjerava utjecaj na težinu usklađivanja s Uredbom i dio u kojem je provjereno koliko posjedovanje ISO/IEC 27001 pomaže u organizaciji poslovanja. Kako se u oba dijela promatra utjecaj posjedovanja ISO certifikata, uvodno je dan pregled o posjedovanju ISO certifikata u organizacijama.

Utvrđeno je da 52,5 % organizacija ima jedan ili više ISO certifikata, pri čemu je najviše organizacija koje imaju jedan certifikat (25,9 %).

Tablica 24. Posjedovanje ISO certifikata: Broj certifikata koje organizacije koriste

Broj ISO sustava	Broj organizacija	%
Nemaju ISO sustav(e)	**66**	**47,5**
Imaju ISO sustav(e)	**73**	**52,5**
1 ISO sustav	36	25,9
2 ISO sustava	19	13,7
3 ISO sustava	13	9,4
4 ISO sustava	1	0,7
5 ISO sustava	4	2,9
Ukupno	**139**	**100,0**

ISO 9001 je najraširenija certifikat, posjeduje ga 38,1 % organizacija, a slijede ISO/IEC 27001 koji posjeduje 27,3 % organizacija i ISO 14001 certifikat koji posjeduje 19,4 % organizacija.

Tablica 25. Posjedovanje ISO certifikata unutar organizacija

ISO sustavi	Broj organizacija	%
ISO 9001	53	38,1
ISO 14001	27	19,4
ISO/IEC 27001	38	27,3
ISO 50001	8	5,8
ISO 45001	1	7,9
Ukupno	**139**	**100,0**

U kontekstu utjecaja posjedovanja ISO certifikata na organizaciju poslovanja provjereno je u kojoj mjeri ispitanici zaposleni u organizacijama koje posjeduju ISO certifikate smatraju da im oni pomažu u organizaciji poslovanja. Testiranje je provedeno neparametrijskim Hi kvadrat testom.

H2.1 Provjera povezanosti percipirane težine uvođenja usklađenosti s Općom uredbom o zaštiti podataka s posjedovanjem ISO certifikata

U nastavku su prikazani rezultati analize utjecaja posjedovanja ISO certifikata na percepciju težine usklađivanja s Općom uredbom o zaštiti podataka.

Direktivnom hipotezom je pretpostavljeno postojanje pozitivnog utjecaja posjedovanja ISO certifikata na implementaciju usklađivanja s Općom uredbom o zaštiti podataka. Testiranje hipoteze provedeno je t-testom za nezavisne uzorke pri čemu su organizacije podijeljene u dvije skupine s obzirom na posjedovanje ISO certifikata. Razlika u prosječnom rezultatu na skali percipirane težine usklađivanja s Uredbom između tako definiranih skupina je statistički značajna (t = 2,292; p = 0,024). Točnije, ispitanici iz skupine organizacija koje posjeduju barem jedan ISO certifikat proces usklađivanja doživljavaju lakšim od onih koji nemaju niti jedan ISO certifikat, čime je direktivna hipoteza potvrđena. Rezultati testiranja prikazani su u Tablici 26.

Tablica 26. Rezultati testiranja razlika u percipiranoj težini usklađivanja s Uredbom s obzirom na posjedovanje ISO certifikata u organizaciji

Percipirana težina usklađivanja		Broj ispitanika	Aritmetička sredina	Std. devijacija	Std. pogreška	t	Stupnjevi slobode	Značajnost p
Posjedovanje ISO certifikata	Imaju ISO sustave	69	3,32	,915	,110	2,292	121	,024
	Nemaju ISO sustave	54	2,94	,878	,119			

Uz testiranje utjecaja posjedovanja ISO sustava općenito na percepciju težine usklađivanja s Uredbom, specifično je testiran i utjecaj korištenja ISO/IEC 27001 u procesu usklađivanja. Prosječan rezultat na skali procjene težine usklađivanja s Uredbom u organizacijama koje koriste ISO/IEC 27001 iznosi 3,56, dok je u organizacijama koje ga ne koriste procjena težine 2,99. Razlika prosječnih rezultata između skupina statistički se značajno razlikuje (t = -3,006; p = 0,004). Rezultati potvrđuju direktivnu hipotezu o facilitirajućem utjecaju korištenja ISO/IEC 27001 pri ispunjavanju zahtjeva propisanih Uredbom. Rezultati testiranja prikazani su u Tablici 27.

Tablica 27. Rezultati testiranja razlika u percipiranoj težini usklađivanja s Uredbom s obzirom na korištenje ISO/IEC 27001 certifikata

Percipirana težina usklađivanja		Broj ispitanika	Aritmetička sredina	Std. devijacija	Std. pogreška	t	Stupnjevi slobode	Značajnost p
Posjedovanje ISO/IEC 27001 certifikata	Imaju ISO/IEC 27001	36	3,56	,998	,166	-3,006	55,923	,004
	Nemaju ISO/IEC 27001	87	2,99	,828	,089			

H2.2 Utjecaj posjedovanja ISO certifikata općenito i ISO/IEC 27001 certifikata na organizaciju poslovanja

U nastavku, u Tablici 28, prikazani su rezultati analize utjecaja posjedovanja ISO certifikata na organizaciju poslovanja. Usporedba dobivene distribucije odgovora na pitanje pomaže li posjedovanje ISO certifikata u organizaciji poslovanja i teorijske (očekivane) distribucije odgovora Hi kvadrat testom pokazuje statistički značajan otklon prema odgovoru „puno pomažu“. S druge strane, broj odgovora „ne pomažu“ je značajno manji od očekivanog (Hi kvadrat = 30,857; P < 0,001). Zaključak je da postojanje ISO sustava pomaže u organizaciji poslovanja, što je u skladu s postavljenom hipotezom.

Tablica 28. Utjecaj posjedovanja ISO certifikata u organizaciji poslovanja

Koliko vam ISO sustav/i koje imate pomaže/u u organizaciji poslovanja?		Dobivena distribucija	Teorijska distribucija	Hi kvadrat	Stupnjevi slobode	Značajnost p
Stupanj pomaganja	Puno pomaže/u	39	21.0	30,857	2	,000
	Donekle pomaže/u	21	21.0			
	Ne pomaže/u	3	21.0			

Nadalje je provjereno u kojoj mjeri ISO/IEC 27001 pomaže u uvođenju Opće uredbe o zaštiti podataka. Testiranje je također provedeno Hi kvadrat testom. Od 32 ispitanika koji su odgovarali na pitanje, samo jedan smatra da ISO/IEC 27001 ne pomaže u situaciji implementacije Uredbe. Dobivena distribucija odgovora je značajno pomaknuta prema odgovoru „puno pomaže“ što potvrđuje postavljenu hipotezu o mogućnosti oslanjanja na ISO/IEC 27001 kod usklađivanja poslovanja organizacija s Općom uredbom o zaštiti podataka. Dobivena razlika u distribuciji odgovora u odnosu na teorijsku distribuciju je statistički značajna (Hi kvadrat = 30,036; P < 0,001), a rezultati testiranja su prikazani u Tablici 29.

Tablica 29. Pomoć ISO/IEC 27001 u usklađivanju s Općom uredbom o zaštiti podataka

Koliko vam ISO/IEC 27001 pomaže ili vam je pomogao u usklađivanju s Općom uredbom o zaštiti podataka?		Dobivena distribucija	Teorijska distribucija	Hi kvadrat	Stupnjevi slobode	Značajnost p
Stupanj pomaganja	Puno pomaže	25	10.7	30,036	2	,000
	Donekle pomaže	6	10.7			
	Ne pomaže	1	10.7			

Zaključci koji slijede iz testiranja Hipoteze 2:

1. Organizacije koje koriste ISO sustave, usklađivanje poslovanja s Općom uredbom o zaštiti podataka percipiraju manje teškim.
2. Organizacije koje koriste ISO sustave u većoj mjeri smatraju kako im to pomaže u poslovanju.
3. Organizacije koje koriste ISO/IEC 27001 u većoj mjeri smatraju kako im to pomaže u uvođenju Opće uredbe o zaštiti podataka.

H3 Utjecaj veličine organizacije i kompleksnosti obrade osobnih podataka na stupanj usklađenosti i način implementacije (raspoloživost ISO sustava, korištenje konzultanata i težina uvođenja)

U sklopu Hipoteze 3 provjereni su odnosi veličine organizacija, podijeljenih na dvije skupine prema broju zaposlenih, s korištenjem ISO sustava, s korištenjem usluga vanjskih konzultanata i percepcijom težine usklađivanja s Općom uredbom o zaštiti podataka. Također, sukladno postavljenoj Hipotezi 3 provjerena je i povezanost kompleksnosti obrade osobnih podataka s korištenjem ISO sustava upravljanja, s korištenjem usluga vanjskih konzultanata kao i s percepcijom težine usklađivanja s Općom uredbom o zaštiti podataka.

Dvije zavisne varijable koje su sadržane u hipotezi, su veličina organizacije i kompleksnost obrade osobnih podataka. Veličina organizacije operacionalizirana je kroz grupiranje organizacija u dvije podjednako velike skupine organizacija prema broju zaposlenih – organizacije koje zapošljavaju manje od 30 osoba i organizacije s 30 i više zaposlenih osoba.

Tablica 30. Podjela organizacija na dvije skupine prema broju zaposlenih

Skupina organizacija prema broju zaposlenih	**Broj organizacija**	**%**
Organizacije s do 29 zaposlenih	69	49,6
Organizacije s 30 ili više zaposlenih	70	50,4
Ukupno	139	100

Druga zavisna varijabla, kompleksnost obrade, operacionalizirana je preko pitanja u upitniku koje se odnosilo na svrhe prikupljanja osobnih podataka – *U koje sve svrhe koristite osobne podatke koje prikupljate?* Ponuđeno je bilo pet odgovora: primarna svrha, vlastite promotivne kampanje, komunikacija nakon kupnje, slanje *newslettera* ili tiskanih materijala i dijeljenje podataka s trećom stranom, a ispitanici su mogli označiti više odgovora. Broj organizacija koje koriste osobne podatke za navedene svrhe prikazan je u tablici. Potrebno je naglasiti da je 40

ispitanika preskočilo odgovoriti na ovo pitanje, tj. nisu željeli na njega dati odgovor, te je stoga ukupan broj ispitanika/organizacija u analizi svrhe korištenja osobnih podataka 99.

Tablica 31. Svrhe korištenja osobnih podataka

Svrha	**Broj organizacija**	**%**
Primarna svrha	93	93,9
Vlastite promotivne kampanje	31	31,3
Komunikacija nakon kupnje	34	34,3
Slanje *newslettera* ili tiskanih materijala	38	38,4
Dijeljenje podataka s trećom stranom	22	22,2
Ukupno	99	100 %

Kako bi se kompleksnost korištenja osobnih podataka kvantificirala i mogla koristiti pri testiranju hipoteza, provedeno je sumiranje broja svrha za koje svaka organizacija koristi osobne podatke. Tako je organizacijama koje osobne podatke koriste u svih pet navedenih svrha, pripisan rezultat 5, organizacijama koje koriste osobne podatke u četiri svrhe, pripisan je rezultat 4, organizacijama koje koriste osobne podatke u tri svrhe, pripisan je rezultat 3, organizacijama koje koriste osobne podatke u dvije svrhe, pripisan je rezultat dva, te organizacijama koje koriste osobne podatke samo u jednu od pet navedenih svrha, pripisan je rezultat jedan. Od svih 99 organizacija koje su odgovorile na ovo pitanje, svaka je navela barem jednu svrhu korištenja osobnih podataka. Distribucija tako dobivenih rezultata stupnja kompleksnosti obrade osobnih podataka prikazana je u Tablici 32.

Tablica 32. Kompleksnost obrade osobnih podataka

Stupanj kompleksnosti obrade podataka (broj svrha korištenja osobnih podataka)	Broj organizacija	%
1 svrha	39	39,4
2 svrhe	22	22,2
3 svrhe	20	20,2
4 svrhe	14	14,1
5 svrha	4	4,0
Ukupno	99	100 %
Prosječan broj svrha obrade osobnih podataka	2,21	
Standardna devijacija broja svrha obrade osobnih podataka	1,223	

U daljnjim je analizama u svrhu testiranja elemenata hipoteze 3, korištena konstruirana varijabla stupnja kompleksnosti obrade osobnih podataka.

H3.1 Povezanost veličine organizacija i korištenja ISO sustava upravljanja

Hipoteza o povezanosti kategorizacije organizacija prema veličini, odnosno prema broju zaposlenih i korištenja ISO sustava upravljanja provjerena je Hi kvadrat testom razlika u distribucijama organizacija s manje od 30 zaposlenih i organizacija s 30 i više zaposlenih s obzirom na korištenje ISO sustava.

Hi kvadrat test neparametrijski je statistički test koji uspoređuje dvije (ili više) distribucija odgovora i utvrđuje statističku značajnost razlika u distribucijama.

Hi kvadrat test povezanosti veličine organizacije i korištenja ISO sustava upravljanja iznosi 14,573 i statistički je značajan ($p < 0,001$).

Kao što je vidljivo iz tablice, organizacije s manjim brojem zaposlenih u statistički značajno većem postotku (63,8 %) ne koriste ISO sustave, za razliku od organizacija s 30 ili više

zaposlenih kod kojih je taj postotak značajno manji (31,4 %), a koje u većem postotku koriste ISO sustave upravljanja (68,6 %).

Prema provedenom statističkom testu, postoji povezanost između veličine organizacije i korištenja ISO sustava upravljanja i to u smjeru prema kojem veće organizacije u većem postotku koriste ISO sustave upravljanja nego manje organizacije.

Tablica 33. Razlike u distribucijama organizacija prema veličini (broju zaposlenih) i korištenja ISO sustava

Organizacije prema veličini (prema broju zaposlenih)		Koriste ISO sustave	Ne koriste ISO sustave	Ukupno
Do 30 zaposlenih	Broj organizacija	25	44	69
	%	36,2 %	63,8 %	100,0 %
30+ zaposlenih	Broj organizacija	48	22	70
	%	68,6 %	31,4 %	100,0 %
Ukupno	Broj organizacija	73	66	139
	%	52,5 %	47,5 %	100,0 %

H3.2 Povezanost veličine organizacija i korištenja vanjskih konzultanata pri usklađivanju s Općom uredbom o zaštiti podataka

Hipoteza o povezanosti veličine organizacija i korištenja vanjskih konzultanata provjerena je, kao i prethodna hipoteza, Hi kvadrat testom. Varijabla o korištenju konzultanata pri usklađivanju s Općom uredbom o zaštiti podataka ima tri stupnja: bez pomoći konzultanata (potpuno samostalno), uz manju pomoć vanjskih konzultanata i uz veću pomoć vanjskih konzultanata.

Hi kvadratom testiralo se distribuiraju li se odgovori na pitanje o korištenju konzultanata jednako unutar organizacija s manje i s više zaposlenih. Vrijednost dobivenog Hi kvadrat testa iznosi 18,047 i statistički je značajna ($p < 0,001$), odnosno postoje razlike u korištenju usluga konzultanata ovisno o veličini organizacije.

U Tablici 34. prikazane su distribucije – brojevi organizacija, kategoriziranih prema veličini, i postotci uz vrijednost *adjusted residual* – korigirani rezidual, koja ukazuje na onu vrijednost (postotak) kod jedne kategorije organizacija koja značajno odstupa od druge kategorije organizacija. Apsolutna vrijednost *adjusted residual* koja se u statistici smatra indikatorom značajne razlike je 2,9 ili više (tj. više od 2,9, odnosno manje od -2,9).

Prema rezultatima prikazanim u tablici vidljivo je kako se manje organizacije (do 30 zaposlenih) u statistički značajno većem postotku odlučuju usklađivati s Općom uredbom samostalno, nego što to čine organizacije s 30 ili više zaposlenih (*adjusted residual* 3,9, odnosno -3,9). Veće se organizacije u statistički značajno većem postotku od manjih organizacija odlučuju i na manju pomoć vanjskih konzultanata (*adjusted residual* 4,0, odnosno -4,0). Kod odgovora – Uz veću pomoć vanjskih konzultanata nije utvrđena statistički značajna razlika između većih i manjih organizacija.

Tablica 34. Razlike u distribucijama organizacija prema veličini (prema broju zaposlenih) i korištenja vanjskih konzultanata pri usklađivanju s Općom uredbom o zaštiti podataka.

Organizacije prema veličini (prema broju zaposlenih)		Potpuno samostalno	Uz manju pomoć vanjskih konzultanata	Uz veću pomoć vanjskih konzultanata	Ukupno
Do 30 zaposlenih	Broj organizacija	34	22	11	67
	%	50,7 %	32,8 %	16,4 %	
	Korigirani rezidual	3,9	-4,0	,5	100,0 %
30+ zaposlenih	Broj organizacija	13	46	9	68
	%	19,1 %	67,6 %	13,2 %	

	Korigirani rezidual	-3,9	4,0	-,5	100,0 %
Ukupno	Broj organizacija	47	68	20	135
	%	34,8 %	50,4 %	14,8 %	100,0 %

Prema provedenom statističkom testu, postoji povezanost između veličine organizacije i korištenja vanjskih konzultanata i to u smjeru češćeg korištenja usluga konzultanata kod većih organizacija, odnosno češćeg samostalnog usklađivanja s Uredbom kod manjih organizacija.

H3.3 Povezanost veličine organizacija i percepcije težine usklađivanja s Općom uredbom o zaštiti podataka

Razlika u percepciji težine usklađivanja s Općom uredbom o zaštiti podataka između manjih i većih organizacija provjerena je t-testom za nezavisne uzorke.

Kao što je vidljivo iz rezultata statističkog testiranje (t = 0,310, p = 0,757), nije potvrđena statistički značajna razlika u percepciji težine usklađivanja s Općom uredbom o zaštiti podataka između manjih i većih organizacija.

Tablica 35. Rezultati testiranja razlika u percipiranoj težini usklađivanja s Uredbom s obzirom na veličinu organizacije

Percipirana težina usklađivanja		Broj ispitanika	Aritmetička sredina	Std. devijacija	Std. pogreška	t	Stupnjevi slobode	Značajnost p
Veličina organizacije	Do 30 zaposlenih	81	3,18	,904	,116	,310	121	,757
	30 ili više zaposlenih	42	3,13	,932	,118			

Tvrtke, neovisno o veličini, podjednako percipiraju težinu usklađivanja s Uredbom.

H3.4 Povezanost kompleksnosti obrade osobnih podataka i korištenja ISO sustava upravljanja

Razlike između organizacija koje koriste ISO sustave upravljanja i tvrtki koje ih ne koriste prema stupnju kompleksnosti obrade osobnih podataka testirane su t-testom za nezavisne uzorke.

Rezultati statističkog testiranja utvrdili su postojanje statistički značajne razlike u kompleksnosti obrade osobnih podataka između organizacija koje koriste ISO sustave i onih koje ga ne koriste (t = 2,431, p = 0,017).

Tablica 36. Rezultati testiranja razlika u kompleksnosti obrade osobnih podataka s obzirom na korištenje ISO sustava

Kompleksnost obrade osobnih podataka		Broj ispitanika	Aritmetička sredina	Std. devijacija	Std. pogreška	t	Stupnjevi slobode	Značajnost p
Korištenje ISO sustava	Koriste ISO sustave	52	2,50	1,291	,179	2,431	96	,017
	Ne koriste ISO sustave	46	1,91	1,071	,158			

Organizacije koje koriste ISO sustave imaju statistički značajno viši stupanj kompleksnosti obrade osobnih podataka.

H3.5 Povezanost kompleksnosti obrade osobnih podataka i korištenja vanjskih konzultanata pri usklađivanju s Općom uredbom o zaštiti podataka.

Razlike između organizacija koje koriste različiti stupanj usluge vanjskih konzultanata (ne koriste, koriste manju pomoć konzultanata i koriste veću pomoć konzultanata) prema

kompleksnosti obrade osobnih podataka, testirana je statističkim testom jednostavne analize varijance (ANOVA).

Preduvjet je za provedbu analize varijance jednaka varijanca odgovora unutar svake od tri skupine prema korištenju usluga konzultanata. Leveneovim testom homogenosti varijance (0,035, p = 0,966) utvrđeno je kako se varijance statistički ne razlikuju, što dopušta provedbu analize varijance.

Tablica 37. Rezultati testiranja razlika u kompleksnosti obrade osobnih podataka s obzirom na korištenje usluga konzultanata pri usklađivanju s Općom uredbom o zaštiti podataka.

Kompleksnost obrade osobnih podataka		Broj ispitanika	Aritmetička sredina	Std. devijacija	Std. pogreška	F	Stupnjevi slobode	Značajnost p
Korištenje usluga konzultanata	Ne koriste	38	2,03	1,262	,205	1,464	2; 93	0,237
	Manja pomoć konzultanata	44	2,48	1,171	,177			
	Veća pomoć konzultanata	14	2,14	1,231	,329			

Analizom varijance utvrđeno je da između skupina organizacija s različitim stupnjem korištenja usluga konzultanata ne postoji statistički značajna razlika u kompleksnosti obrade osobnih podataka (F = 1,464, p = 0,237). Kako F vrijednost, odnosno razlike među skupinama nisu statistički značajne, nisu se provodili *post-hoc* testovi usporedbi parova skupina ispitanika.

H3.6 Povezanost kompleksnosti obrade osobnih podataka i percepcije težine uvođenja usklađenosti s Općom uredbom o zaštiti podataka.

Povezanost kompleksnosti obrade osobnih podataka i percepcije težine usklađenosti provedena je bivarijatnom korelacijskom analizom jer su obje varijable na kontinuiranim dimenzijama. Korišten je Pearsonov koeficijent korelacije r.

Tablica 38. Povezanost kompleksnosti obrade osobnih podataka i percepcije težine uvođenja sukladnosti s Općom uredbom o zaštiti podataka.

		Proces usklađivanja s Općom uredbom o zaštiti podataka u Vašu organizaciju biste opisali kao*
Kompleksnost obrade osobnih podataka	Pearson r	,143
	Značajnost p	,185
	Broj ispitanika	87

Kao što je vidljivo iz niskog koeficijenta korelacije, koji se nije pokazao statistički značajnim (r = 0,143, p = 0,185), nije utvrđena povezanost između kompleksnosti obrade osobnih podataka i percepcije težine usklađivanja s Općom uredbom o zaštiti podataka.

Zaključci koji slijede iz testiranja Hipoteze 3:

1. Veće organizacije češće koriste ISO sustave upravljanja.
2. Manje organizacije češće samostalno provode usklađivanje s Općom uredbom o zaštiti podataka.
3. Organizacije neovisno o veličini podjednako percipiraju težinu usklađivanja s Uredbom.
4. Organizacije koje koriste ISO sustave imaju viši stupanj kompleksnosti obrade osobnih podataka.
5. Ne postoji povezanost između kompleksnosti obrade osobnih podataka i korištenja usluga konzultanata.
6. Ne postoji povezanost između kompleksnosti obrade osobnih podataka i percipirane težine usklađivanja s Općom uredbom o zaštiti podataka.

Dodatna pitanja o poslovanju sa zemljama Europske unije

Neusklađenost organizacija s Općom uredbom o zaštiti podataka može rezultirati nepovoljnim posljedicama prvenstveno u aspektu nemogućnosti izvoza na europsko tržište, a osobito Jedinstveno digitalno tržište (DSM) kod *online* plasmana proizvoda i usluga.

Na pitanje o sadašnjem poslovanju sa zemljama Europske unije, odnosno izvozu u zemlje EU-a, 33,7 % ispitanika odgovorilo je da ne posluje sa zemljama EU, kod 24,2 % na izvoz u EU se odnosi 10 % i manje prihoda dok kod preostalih 42,1 % na izvoz u EU otpada više od 10 % prihoda. Razlike između skupina s obzirom na stupanj usklađenosti s Općom uredbom o zaštiti podataka, nisu statistički značajne.

Tablica 39. Stupanj usklađenosti s Općom uredbom o zaštiti podataka i poslovanje sa zemljama Europske unije

Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?		Postotak prometa (izvoza) u EU			
		Ne posluju s EU-om	Malo posluju (do 10 % prihoda)	Više posluju s EU-om (više od 10 % prihoda)	**Ukupno**
Da, u potpunosti smo uskladili	Broj ispitanika	22	16	29	**67**
	% Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?	32,8 %	23,9 %	43,3 %	**100,0 %**
Proces usklađivanja je u tijeku	Broj ispitanika	7	6	7	**20**
	% Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?	35,0 %	30,0 %	35, 0%	**100,0 %**
Planiramo usklađivanje s Općom uredbom o zaštiti podataka	Broj ispitanika	3	1	3	**7**
	% Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?	42,9 %	14,3 %	42,9 %	**100,0 %**
Ukupno	Broj ispitanika	**32**	**23**	**40**	**95**
	% Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?	**33,7 %**	**24,2 %**	**42,1 %**	**100,0 %**

Zanimljivo je da 33,7 % ispitanika smatra da će njihove organizacije u tekućoj godini povećati udio vrijednosti poslovanja sa zemljama EU-a te da je takav trend prisutan i u organizacijama koje do sada nisu u potpunosti uskladile poslovanje s Općom uredbom o zaštiti podataka. Naime, u organizacijama u kojima je proces usklađivanja još u tijeku i onima koje planiraju pokrenuti proces usklađivanja s Uredbom, trećina (33,3 %) očekuje povećanje udjela vrijednosti poslovanja sa zemljama Europske unije u svojim prihodima iako još uvijek nisu ispunile nužan uvjet o usklađivanju s Općom uredbom o zaštiti podataka.

7. Zaključak

Europsko je Jedinstveno digitalno tržište (DSM), zahvaljujući e-trgovini i e-upravi, jedan od najvažnijih pokretača europskog gospodarstva. Zbog značajnih promjena uvjetovanih novim načinom pružanja usluga ili plasmana proizvoda uslijed digitalne transformacije poslovanja donesen je regulatorni okvir koji ne ovisi o državnim granicama i usmjeren je ka zaštiti privatnosti te informacijskoj i kibernetičkoj sigurnosti.

Europski zakoni odnosno direktive i uredbe vezane uz zaštitu osobnih podataka, kao opći normativni tekstovi ne nude procesno primjenjiv način usklađivanja organizacija s njihovim zahtjevima što je vidljivo u otežanom razumijevanju organizacija oko nužnih prilagodbi organizacijskih, ali i tehničkih aspekata u poslovanju. Uz pravne posljedice, neusklađenost s regulativom dovodi i do značajnih posljedica u smislu otežavanja ili potpune nemogućnosti daljnjeg izvoza na europsko tržište i plasmana na Jedinstveno digitalno tržište.

Međunarodni ISO/IEC standardi predstavljaju pregled globalnih najboljih praksi u različitim područjima. Europska komisija u svojim recentnim dokumentima ukazuje na snažnu usmjerenost Europske unije ka sve opsežnijoj regulaciji i standardizaciji usluga i proizvoda vezanih uz digitalni protok podataka te prvi put službeno ukazuje na konvergentnost ISO standarda u svojstvu zaštite sustava i podataka, osobito osobnih podataka, spominjući pritom i standarde ISO/IEC 27001 i ISO/IEC 27701.

Ova disertacija ima dva osnovna cilja koji su ispunjeni odnosno (1) utvrditi utječe li izostanak modela primjene na proces implementacije usklađenosti s Uredbom i u kojoj bi mjeri korištenje bazne metodologije ISO/IEC 27001 standarda u formiranju modela primjene facilitiralo usklađivanje poslovnih procesa organizacija s Uredbom te (2) izraditi model za prepoznavanje konteksta obrada osobnih podataka u menadžmentu poslovnih procesa i načinu provođenja njihovog usklađivanja s Uredbom i nacionalnim provedbenim zakonom ili revizije usklađenosti.

Primarnim istraživanjem ustanovljena je međupovezanost između (1) razumijevanja zahtjeva propisanih Općom uredbom o zaštiti podataka (Uredba EU 2016/679) i (2) nedostatka

smjernica za usklađivanje poslovnih procesa s Uredbom te je ustanovljena i orijentiranost plasmanu na europsko tržište. Dobiveni rezultati pokazali su da je većina ispitanika razumjela obveze propisane Uredbom (njih ukupno 91,8 %) no čak 41,5 % njih je imalo potrebu za dodatnim stručnim pojašnjenjima, a čak 9,2 % njih nije razumjelo nove obveze. Također, pokazalo se da organizacije koje u svom poslovanju koriste ISO sustave, usklađivanje s Uredbom percipiraju manje teškim, a one koje koriste ISO/IEC 27001 smatraju u većoj mjeri kako im to pomaže u ispunjenju zahtjeva propisanih Uredbom. Nije ustanovljena povezanost između veličine organizacije, kompleksnosti obrade osobnih podataka i percipirane težine usklađivanja s Uredbom, ali je značajno da se na čak 24,2 % ispitanika izvoz u EU odnosi 10 % i manje prihoda dok kod preostalih 42,1 % na izvoz u EU otpada više od 10 % prihoda, a pritom među njima nema statistički značajnih razlika s obzirom na stupanj njihove usklađenosti s Uredbom. Istovremeno 33,7 % ispitanika smatra da će njihove organizacije u tekućoj godini povećati udio vrijednosti poslovanja sa zemljama EU-a te je takav trend prisutan i u organizacijama koje do sada nisu u potpunosti uskladile poslovanje s Uredbom. Naime, u organizacijama u kojima je proces usklađivanja još u tijeku i onima koje tek planiraju pokrenuti proces usklađivanja s Uredbom, trećina (33,3 %) očekuje povećanje udjela vrijednosti poslovanja sa zemljama Europske unije u svojim prihodima iako još uvijek nisu ispunile nužan uvjet o usklađivanju s njome.

NPISPMSA model sustava upravljanja informacijskom sigurnošću i privatnošću predstavlja primjenjiv opći okvir za strukturirano uspostavljanje, usklađivanje i provođenje revizije usklađenosti organizacijskih i tehničkih mjera u menadžmentu poslovnih procesa s Uredbom i nacionalnim provedbenim zakonom i/ili kontrolama proširenog ISO/IEC 27001 sustava upravljanja informacijskom sigurnosti.

Model se može koristiti u (1) analizi stanja usklađenosti organizacijskih i tehničkih mjera sa zahtjevima propisanim Uredbom i/ili (2) analizi usklađenosti postojećeg sustava s kontrolama proširenog ISO/IEC 27001 sustava upravljanja informacijskom sigurnosti u svrhe implementacije i revizije odnosno internog audita, audita druge strane ili certifikacijskog audita (audita treće strane). Mogu ga koristiti organizacije svih vrsta i veličina, javne i privatne, kao i državna tijela te neprofitne organizacije koje su voditelji obrade i/ili izvršitelji obrade osobnih

podataka neovisno o tome imaju li već u svojoj organizaciji uspostavljen sustav upravljanja informacijskom sigurnošću ili posjeduju ISO/IEC 27001 certifikat.

Verifikacijom modela je potvrđeno da dobiveni procesni model zadovoljava postavljene specifikacije odnosno organizacijama olakšava razumijevanje zahtjeva propisanih Uredbom i implementiranje tehničkih i organizacijskih mjera u menadžmentu poslovnih procesa u usklađivanju s ovom zakonskom regulativom; kao i usklađivanje s kontrolama proširenog sustava upravljanja informacijskom sigurnosti standarda ISO/IEC 27001.

Literatura

Knjige i publikacije

1. Agencija Europske unije za temeljna prava i Vijeće Europe (2018). *Priručnik o europskom zakonodavstvu o zaštiti podataka*, Luksemburg: Ured za publikacije Europske unije, doi:10.2811/66223
2. Andrijanić, I. i Pavlović, D. (2016). *Međunarodno poslovanje.* Zagreb: Libertas, Plejada.
3. Andrijanić, I., Gregurek, M. i Merkaš, Z. (2016). *Upravljanje poslovnim rizicima.* Zagreb: Libertas, Plejada.
4. Awad, I.A. i Fairhurst, M. (2018). *Information Security Foundations, technologies and applications*. The Institution of Engineering and Technology, London, Ujedinjeno Kraljevstvo
5. Butković, H. i Samardžija, V. (2019.) *Digitalna transformacija tržišta rada u Hrvatskoj*. Institut za razvoj i međunarodne odnose, Zagreb.
6. Caballero, A. (2014). *Information Security Essentials for IT Managers.* u Vacca, J.R. (Ur). *Managing Information Security*. Elsevier Inc.
7. Calder, A. i Watkins, S. (2008). IT governance : A manager's guide to data security and ISO 27001/ ISO 27002 (4th edition). Kogan Page.
8. Carvalho L.C. i Isaias, P. (2019). *Handbook of research on entrepreneurship and marketing for global reach in the digital economy.* Hershey, PA: IGI Global, Business Science Reference.
9. Dragičević, D. (2015). *Pravna informatika i pravo informacijskih tehnologija*, p. 103 Zagreb: Narodne novine
10. Dragičević, D. (2019). *Pravna informatika i pravo informacijskih tehnologija*, revidirano poglavlje 5: p. 17, Sveučilište u Zagrebu, Pravni fakultet: Zagreb
11. Ervural, B.C. i Ervural B. (2018). *Overview of Cyber Security in the Industry 4.0 Era* u Ustundag, A. i Cevikcan, E. (Ur.). *Industry 4.0: Managing The Digital Transformation*. Springer.
12. Frost and Sullivan (2017). *Cyber Security in the Era of Industrial IoT*. Frost & Sullivan White Paper, Njemačka.

13. Ivanković, Ž. (2018). *Besplatno, Uvod u političku ekonomiju digitalnog doba*. Naklada Jesenski i Turk: Zagreb.
14. James, A. i sur. (2018). Security challenges and solutions for e-business u Awad, A. I. i Fairhurst, M. (Ur.). *Information Security: Foundations, technologies and applications*. The Institution of Engineering and Technology.
15. Kaplan, J., Weinberg, A, i Sharma, S. (2011). *Meeting the cybersecurity challenge*. Digit. McKinsey.
16. Kim, D. i Solomon, M.G. (2016). *Fundamentals of information systems security*. Third edition, Jones & Bartlett Learning, Burlington, Massachusetts, SAD.
17. Kolaković, M. (2006). *Poduzetništvo u ekonomiji znanja.* Zagreb: Sinergija.
18. Kopal, R, Korkut, D. (2020) *Analitički menadžment*. Visoko učilište Effectus – visoka škola za financije i pravo, Zagreb.
19. Kopal, R., Korkut, D. (2014) *Tehnike kompetitivne analize*. Visoko učilište Effectus – visoka škola za financije i pravo, Zagreb; IN2data d.o.o., Zagreb.
20. Kotler, P; Kartajaya, H; Setiawan, I (2017). *Marketing 4.0 – Moving from Traditional to Digital*, John Wiley & Sons, Inc., Hoboken, New Jersey.
21. Ladley, J. (2012). *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program*. Elsevier.
22. Landoll, D.J. (2016). *Information security policies, procedures, and standards.* CRC Press.
23. Lazibat, T. i Kolaković, M. (2004). *Međunarodno poslovanje u uvjetima globalizacije.* Zagreb: Sinergija.
24. Maliki, T. i Seigneur, J. (2014). *Online Identity and User Management Services u* u Vacca, J.R. (Ur). *Managing Information Security*. Elsevier Inc.
25. Mallery, J.R. (2017). *Building a Secure Organization.* u Vacca, J.R. (Ur). *Computer and Information Security Handbook*. Elsevier Inc.
26. Milanja, C. (2012.) *Konstrukcije kulture*. Zagreb: Institut društvenih znanosti Ivo Pilar.
27. Moore, A. (2018). *The GDPR & Managing Data Risk*, Symantec Special Edition. John Wiley & Sons, Ltd., Chichester, West Sussex, UK
28. Oswald, G. i Kleinemeier (2016). *Shaping the Digital Enterprise: Trends and Use Cases in Digital Innovation and Transformation*. Springer.

29. Pejić Bach, M., Spremić, M. i Suša Vugec, D. (2017). *Integrating Digital Transformation Strategies into Firms: Values, Routes and Best Practice Examples*. Management and Technological Challenges in the Digital Age /Novo Melo, P.; Machado, C.(eds.). Boca Raton, Florida: Taylor & Francis Group: CRC press, pp. 107-128
30. Petersen, S. V. (2003). *A Critical Rewriting of Global Political Economy: Integrating Reproductive, Productive, and Virtual Economies.* London: Routledge, UK.
31. Pooley, J. (2017). *Information Security in the Modern Enterprise* u Vacca, J.R. (Ur). *Computer and Information Security Handbook.* Elsevier Inc.
32. Rogers, D. L. (2016). *The digital transformation playbook: Rethink your business for the digital age.* Columbia University Press.
33. Salkin, C., Oner, M., Ustundag, A. i Cevikcan, E. (2018). A Conceptual Framework for Industry 4.0. u Ustundag, A. i Cevikcan, E. (Ur.). *Industry 4.0: Managing The Digital Transformation*. Springer.
34. Samuelson, P.A.; Nordhaus, W.D. (2005) *Ekonomija*, 18. izdanje. Mate: Zagreb.
35. Schreckling, E. i Steiger, C. (2016). *Digitalize or Drown* u Gerhard Oswald i Michael Kleinemeier (2016). Shaping the Digital Enterprise. Springer.
36. Smith, Adam, 1723-1790. (1994). *An inquiry into the nature and causes of the wealth of nations*. New York : Modern Library
37. Spremić, M. (2017). *Digitalna transformacija poslovanja*. Sveučilište u Zagrebu, Ekonomski fakultet: Zagreb.
38. Thapa, D., Fumudoh, S. i Vishwanathan, U. (2018). *Information systems security issues in the context of developing countries* u Awad, A. I. i Fairhurst, M. (Ur.). *Information Security: Foundations, technologies and applications*. The Institution of Engineering and Technology.
39. Tolstoguzov, O. i Pitukhina, M. (2020). *Migration and Urbanization: Local Solutions for Global Economic Challenges*. IGI Global.
40. Vacca, J.R. (2017). *Computer and Information Security Handbook.* Third edition. Elsevier.
41. Vukelić, B. (2016). *Sigurnost informacijskih sustava*. Veleučilište u Rijeci, Rijeka.
42. Whitman, M.E. i Mattord H.J. (2018). *Principles of Information Security, Sixth Edition.* Cengage Learning.

Znanstveni i stručni članci

1. Aksentijević, S. (2014). *Model ekonomski održivog sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima* : doktorska disertacija (Disertacija). Preuzeto s https://www.bib.irb.hr/856967
2. Bloomberg, J. (2018). *Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril*, Forbes. Dostupno na: https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/?sh=7e003c0b2f2c, pristupljeno 24.12.2020.
3. Bratranek, N., Kopal, R. (2008). *Uvođenje poreznog broja: upravljanje identitetom poreznih obveznika i zaštita osobnih podataka*, Zbornik Visoke poslovne škole Libertas, Zagreb, 1(1), ISSN:1846-9728, UDK 004.056:658.5, p. 380-388.
4. Calvino, F., et al. (2018). *A taxonomy of digital intensive sectors*, OECD Science, Technology and Industry Working Papers, No. 2018/14, OECD Publishing, Paris, https://doi.org/10.1787/f404736a-en.
5. Campolargo, M. (2011). *e-Infrastructures for Science in the Digital Age*. Europska komisija, Emerging Technologies and Infrastructures. Dostupno na: https://science.osti.gov/-/media/ascr/ascac/pdf/meetings/aug11/Campolargo.pdf , pristupljeno 11.11.2020.
6. Charif B., and Awad A.I. (2016). *Towards smooth organisational adoption of cloud computing a customer-provider security adaptation*. Computer Fraud&Security. 2016(2):7–15. doi: http://dx.doi.org/10.1016/S1361-3723(16)30016-1.
7. Charif B., Awad A.I. (2014). *Business and Government Organizations' Adoption of Cloud Computing.* Intelligent Data Engineering and Automated Learning – IDEAL 2014, ur. Corchado E., Lozano J.A., Quintián H., and Yin H., 15th International Conference, Salamanca, Španjolska, 10–12.9.2014. Zbornik radova. pp. 492–501. Springer International Publishing, Cham. doi: https://doi.org/10.1007/978-3-319-10840-7_59.
8. Daidj, N (2019). *Strategic and Business-IT Alignment Under Digital Transformation: Towards New Insights?*. U Business Transformations in the Era of Digitalization. IGI Global, Business Science Reference.

9. Floridi, L. (2018). *Soft Ethics and the Governance of the Digital*, Philosophy & Technology, 3/2018, sv.31, br.1, str.1–8.
10. Goldfarb, A. i Tucker, C. (2017). *Digital Economics*. NBER Working, Paper No. 23684. Dostupno na: http://www.nber.org/papers/w23684, pristupljeno 10.11.2020.
11. Grzenda M., Furtak J., Legierski J., Awad A.I. (2017). *Network Architectures, Security, and Applications: An Introduction. Advances in Network Systems: Architectures, Security, and Applications*. pp. 1–10. Springer International Publishing. Cham. doi: https://doi.org/10.1007/978-3-319-44354-6_1.
12. Guerra Guerra, A.; Sánchez de Gómez, L.; Jurado Rivas, C. (2019). *Digital Social Innovation: Fundamentals and Framework of Action.* Organizational Transformation and Managing Innovation in the Fourth Industrial Revolution, IGI Global. DOI: 10.4018/978-1-5225-7074-5.ch010
13. Gumzej, N. (2017). *Uredba o zaštiti osobnih podataka*. 2-3. Znanstveni. Zagreb : Pravni fakultet. Dostupno na: https://www.bib.irb.hr/951269, pristupljeno 17.01.2021.
14. Hyder, S. (2020). *B2B eCommerce: Here's What Every B2B Company Needs to Know*. Forbes. Dostupno na: https://www.forbes.com/sites/shamahyder/2020/01/02/b2b-ecommerce-heres-what-every-b2b-company-needs-to-know/#176fb8661271, pristupljeno 31.7.2020.
15. Igrec, A. (2018.) *Digitalna transformacija*. Završni rad. Sveučilište u Zagrebu, Fakultet organizacije i informatike: Varaždin. Dostupno na: https://repozitorij.foi.unizg.hr/islandora/object/foi%3A3889/datastream/PDF/view, pristupljeno 05.11.2020.
16. Kasahara, P. (2018). *Transform today to thrive tomorrow: Leading a Bionic Transformation*, PwC Švicarska, dostupno na: https://www.pwc.ch/en/insights/strategy/leading-a-bionic-transformation.html, pristupljeno 28.11.2020.
17. Kelmanson, B., Kirabaeva, K., Medina, l., Mircheva, B., Weiss, J. (2019). Explaining the Shadow Economy in Europe: Size, Causes and Policy Options, IMF Working Paper WP/19/278.
18. King J. i Awad A.I. (2016). *A distributed security mechanism for resourceconstrained IoT devices*. 40(1):133–143, Informatica, Slovenija.

19. Klaić, A. (2006). *Information Security Requirements in the Information Systems Planning Process*. 17th IIS Conference, FOI, Varaždin, p. 265-269
20. Kopal, R., Pedišić, V. (2008). *Sustav upravljanja informacijskom sigurnošću*, Zbornik Visoke poslovne škole Libertas, Zagreb, 1(1), ISSN:1846-9728, UDK 004.056:658.5, p. 177-184.
21. Kowalkiewicz, M., Safrudin, N., i Schulze, B. (2016). *The Business Consequences of a Digitally Transformed Economy* u Oswald, G. i Kleinemeier, M. (Ur.). Shaping the Digital Enterprise: Trends and Use Cases in Digital Innovation and Transformation. Springer.
22. Liu, D.Y.; Chen, S.W.; Chou, T.C. (2011). *Resource fit in digital transformation: lessons learned from CBC global e-banking project*. Management Decision, Vol. 49, Issue 10.
23. Lundgren, B., Möller, N. (2019). *Defining Information Security*. Sci Eng Ethics 25, 419–441. doi: https://doi.org/10.1007/s11948-017-9992-1
24. McMillan, S. J., Downes, E. J. (2000). *Defining interactivity: a qualitative identification of key dimensions*. New Media & Society, Vol 2 No 2, pp 157–179. Palgrave Macmillan, Cham
25. Mikić, M., Primorac, D. i Kozina, G. (2016). Determining the link between internationalization and business performance of SMEs. *Tehnički vjesnik/Technical Gazette, 23*(4), str. 1201-1206.
26. Morrar, R., Arman, H. & Mousa, S. (2017). *The Fourth Industrial Revolution (Industry 4.0): A Social Innovation Perspective*, Technology Innovation Management Review, 7(11)
27. Nikolić, G., Parlov, N., Sičaja, Ž. (2018). *GDPR - Analysis of pre-representation of small and medium-size businesses to the new european regulation and its future impact on business*. PILC 2018: From Entrepreneur to Leader, Conference Proceedings, ISBN: 978-953-59508-20-0, UDK 349.2:334.71
28. Parlov, N., Perkov, D., Sičaja, Ž. (2016). *New trends in tourism destination branding by means of digital marketing*. Acta Economica Et Turistica, 2(2). doi:10.1515/aet-2016-0012

29. Parlov, N., Sičaja, Ž., Katulić, T. (2018). *GDPR – Impact of General Data Protection Regulation on Digital Marketing. Annals of Disaster Risk Sciences*, 1 (2), 105-116. Preuzeto s https://hrcak.srce.hr/212766
30. Pihir, I., Tomičić-Pupek, K., Tomičić Furjan, M. *Digital Transformation.* Proceedings of the Central European Conference on Information and Intelligent Systems. 29th CECIIS, rujan 19-21, 2018.
31. Rodrigues, R., Barnard-Wills, D., De Hert, P., Papakonstantinou, V. (2016). *The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR*, International Review of Law, Computers & Technology, doi: 10.1080/13600869.2016.1189737
32. Romanelli, M. (2019). *Towards Sustainable Peace by Technology*. Marketing Peace for Social Transformation and Global Prosperity, IGI Global. DOI: 10.4018/978-1-5225-7464-4.ch005
33. Rustici, C. (2018). *GDPR Profiling and Business Practice*, University of Sussex Library, CRi 2/2018, Sussex, p. 34-43
34. Sabolić, D. (2013). *Rizik i nesigurnost I. Rizik i njegovo mjerenje; sklonost ka riziku*. Inženjerska ekonomika, bilješke s predavanja. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb. Dostupno na: https://bib.irb.hr/datoteka/629658.Inzeko10a_Rizik_i_nesigurnost_I_130511.pdf, pristupljeno 10.01.2021.
35. Sesvečan. V. (2005). *Certifikat za ISO 27001 u Hrvatskoj imaju samo dvije tvrtke*, Poslovni dnevnik. Dostupno na https://www.poslovni.hr/sci-tech/certifikat-za-iso-27001-u-hrvatskoj-imaju-samo-dvije-tvrtke-372, pristupljeno 14.7.2020.
36. Seth, A., Wadhawan, N., (2016). *Technology Revolutionizing Retail Practices in Digital Era*. International Journal of Recent Research Aspects, 60-62.
37. Shahjee, R., (2016). *The Impact Of Electronic Commerce On Business Organization*. Scholarly Research Journal for Interdisciplinary Studies. 4 (27), 3130-3140.
38. Shettar, M., (2016). *Emerging Trends of E-Commerce in India: An Empirical Study. International Journal of Business and Management Invention*. 5 (9), 25-31.
39. Sicilia, M., Ruiz, S., Munuera, J. L. (2005). Eff*ects of interactivity in a web site: the moderating effect of need for cognition*. Journal of Advertising, Vol 34 No 3, pp 31–45.

40. Spremić, M.; Hlupić, V. (2007). *e-Commerce in Croatia*, Information Technology for Development, Vol. 14, Num. 4.
41. Strømmen-Bakhtiar, A. (2019). *Digital Economy, Business Models, and Cloud Computing*. U Global Virtual Enterprises in Cloud Computing Environments. IGI Global, Business Science Reference.
42. Strømmen-Bakhtiar, A. (2019). *Digital Economy, Business Models, and Cloud Computing*. Global Virtual Enterprises in Cloud Computing Environments, IGI Global. DOI: 10.4018/978-1-5225-3182-1.ch002
43. Tolstykh, T., Yulia Vertakova, Y. i Shkarupeta, E. (2020). *Handbook of Research on Students' Research Competence in Modern Educational Contexts.* IGI Global. p. 518.
44. Tunjić, D.; Kozina, G.; Primorac, D. (2016). *Certification efficiency of quality management system in metal-processing industry according to standard ISO 9001 in the Republic of Croatia.* 12. međunarodna konferencija ekonomskog i društvenog razvoja, Zbornik radova. 174-180. Varaždin: VADEA
45. Valarmathy, V., Sasanga, U., Sujit Kumar, S., Kavya, S., 2018. *A comparative study of e-commerce business models*. International Research Journal of Engineering and Technology. Vol. 05 Iss. 03.
46. Wadhawan, N. i Arya, R.K. (2020). *Understanding e-commerce: A study with reference to competitive economy.* Journal of Critical Reviews. Vol 7, Issue 8.
47. Ziegler S., Evequoz E., Huamani A.M.P. (2019). *The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities*. In: Aagaard A. (eds) Digital Business Models.

Zakoni, standardi i službene objave

1. Burt, D. (2020) *Microsoft: Azure is now certified for the ISO/IEC 27701 privacy standard*. Microsoft. Dostupno na: https://azure.microsoft.com/en-us/blog/azure-is-now-certified-for-the-iso-iec-27701-privacy-standard/, pristupljeno 17.1.2021.
2. CB Insights (2019). *Research Report: The Future Of Data Security*. Dostupno na: https://www.cbinsights.com/research/report/data-security-future-technologies/, pristupljeno 09.09.2020.

3. CB Insights (2020). *2020 Cyber Defenders: This year's trends, opportunities, and high-momentum startups with the potential to shape the future of cybersecurity*. *https://www.cbinsights.com/research/report/data-security-future-technologies/.*
4. DZS (2018). *Primjena informacijskih i komunikacijskih tehnologija (IKT) u poduzećima u 2018., prvi rezultati.* https://www.dzs.hr/Hrv_Eng/publication/2018/02-03-01_01_2018.htm
5. DZS (2019). *Primjena informacijskih i komunikacijskih tehnologija (IKT) u poduzećima u 2019., prvi rezultati.* https://www.dzs.hr/Hrv_Eng/publication/2019/02-03-01_01_2019.htm
6. Eurofound (2020). *European Working Conditions Survey - Data visualisation*. Dostupno na https://www.eurofound.europa.eu/data/european-working-conditions-survey, pristupljeno 19.11.2020.
7. European Comission (2020). *Digital Scoreboard: Digital Economy and Society Index*. Dostupno na: https://digital-agenda-data.eu/datasets/desi/indicators, pristupljeno 10.01.2021.
8. Europska komisija (2011). *A European strategy for smart, sustainable and inclusive growth.* https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf.
9. Europska komisija (2011). *Europe 2020: A European strategy for smart, sustainable and inclusive growth*. Dostupno na: https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf, pristupljeno 28.12.2020.
10. Europska komisija (2016). *Economic Study on Consumer Digital Content Products - Final Report*. Dostupno na: https://ec.europa.eu/info/sites/info/files/study-consumer-digital-content-products_en.pdf, pristupljeno 18.09.2020.
11. Europska komisija (2018). Republika Hrvatska, Ministarstvo Uprave: *Pismo povjerenici Europske komisije s informacijama o stupanju na snagu nacionalnog provedbenog zakona*. Dostupno na: https://ec.europa.eu/info/sites/info/files/hr_notification_art_51.4_84.2_85.3_88.3_90.2_publish_0.pdf, pristupljeno 11.8.2020.

12. Europska komisija (2020), *Standard contractual clauses for data transfers between EU and non-EU countries*. Dostupno na: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, pristupljeno 18.08.2020.
13. Europska komisija (2020). *Digital Economy and Society Index (DESI) 2020 Questions and Answers.* https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1022.
14. Europska komisija (2020). *Digital Economy and Society Index (DESI) 2020*. Dostupno na: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1022m, pristupljeno 10.01.2021.
15. Europska komisija (2020). *Digital Economy and Society Index (DESI) 2020 Questions and Answers*. Dostupno na: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1022, pristupljeno 28.12.2020.
16. Europska komisija (2020). *E-Commerce directive*. Dostupno na: https://ec.europa.eu/digital-single-market/en/e-commerce-directive, pristupljeno 17.12.2020.
17. Europska komisija (2020). Eurostat, *E-commerce statistics*, Dostupno na: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics , pristupljeno 2.9.2020.
18. Europska komisija (2020). Eurostat, *Statistics on ICT usage and e-commerce introduced*. Dostupno na: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_ICT_usage_and_e-commerce_introduced, pristupljeno 02.09.2020.
19. Europska komisija (2020). *Indeks gospodarske i društvene digitalizacije (DESI) za 2020*.https://mmpi.gov.hr/UserDocsImages/dokumenti/PROMET/Promet%206_19/DESI2019-Croatia-Country-Report%20HR%2011-6_19.pdf
20. Europska komisija (2020). *Rolling plan for ICT standardisation 2020*. Dostupno na https://ec.europa.eu/docsroom/documents/41541, pristupljeno 28.12.2020.
21. Europska komisija (2020). *Shaping Europe's digital future*. Dostupno na: https://ec.europa.eu/digital-single-market/en, pristupljeno 17.12.2020.

22. Europska komisija (2020). *Shaping Europe's digital future*. Dostupno na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en, pristupljeno 10.01.2021.
23. Europska komisija (2020). *SME Strategy: Internal Market, Industry, Entrepreneurship and SMEs*. Dostupno na: https://ec.europa.eu/growth/smes/sme-strategy_en, pristupljeno 10.01.2021.
24. Europska komisija (2020). *The Digital Services Act package*. Dostupno na: https://ec.europa.eu/digital-single-market/en/digital-services-act-package, pristupljeno 17.12.2020.
25. Europska komisija (2020). *The European Digital Strategy*. Dostupno na: https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy, pristupljeno 11.8.2020.
26. Europska komisija (2020). *The European Digital Strategy*. Dostupno na: https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy, pristupljeno 11.8.2020.
27. Europska komisija (2020). *White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust*. Dostupno na: https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence, pristupljeno 10.09.2020.
28. Europska komisija (2020c). *Shaping Europe's digital future*. Dostupno na: https://ec.europa.eu/digital-single-market/en, pristupljeno 17.12.2020.
29. Europska unija (2016). *Povelja Europske unije o temeljnim pravima* (2016/C 202/02). Službeni list Europske unije. Br. 202:389-405. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:12016P/TXT&from=RO , pristupljeno 12.11.2020.
30. Europski fond za regionalni razvoj (2020). *Project Future Ecom: State of the Art Report E-Sales & Marketing*. Dostupno na: https://www.interregeurope.eu/fileadmin/user_upload/tx_tevprojects/library/file_1586338838.pdf , pristupljeno 23.8.2020.
31. Europski parlament (2020). *Četiri nove pogodnosti za potrošače*. Dostupno na: https://www.europarl.europa.eu/news/hr/headlines/economy/20190117STO23721/cetiri-nove-pogodnosti-za-potrosace, pristupljeno 17.9.2020.

32. Europski parlament (2020). *Ugovor iz Lisabona*. Informativni članci o Europskoj uniji. Dostupno na: https://www.europarl.europa.eu/factsheets/hr/sheet/5/ugovor-iz-lisabona , pristupljeno 11.11.2020.
33. Europski parlament. (2020). *Digital Agenda for Europe 2020*. Dostupno na: https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.3.pdf, pristupljeno 29.12.2021.
34. Europsko vijeće, Vijeće Europske unije (2020) *Jedinstveno digitalno tržište za Europu*. Dostupno na https://www.consilium.europa.eu/hr/policies/digital-single-market/, pristupljeno 26.1.2020. godine.
35. Europsko vijeće, Vijeće Europske unije (2020). *Jedinstveno digitalno tržište za Europu*. Dostupno na https://www.consilium.europa.eu/hr/policies/digital-single-market/, pristupljeno 26.1.2020. godine.
36. Europsko vijeće, Vijeće Europske unije (2020.) *Jedinstveno digitalno tržište za Europu*. Dostupno na https://www.consilium.europa.eu/hr/policies/digital-single-market/, pristupljeno 26.1.2020. godine.
37. Eurostat (2019a). *Digital economy and society statistics – enterprises*. https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_enterprises.
38. Eurostat (2019b). Smarter, greener, more inclusive? Indicators to support the Europe 2020 strategy. 2019 Edition. Eurostat https://ec.europa.eu/eurostat/documents/3217494/10155585/KS-04-19-559-EN-N.pdf/b8528d01-4f4f-9c1e-4cd4-86c2328559de
39. Fipra International (2020). *The EU'sDigital Agenda: in light of COVID-19*. Dostupno na: https://www.cabinet-samman.com/files/item/Digital%20look%20at%20the%20EU%20Digital%20agenda%20in%20light%20of%20COVID19%20-%2021%20April%202020.pdf, pristupljeno 15.12.2020.
40. International Organization for Standardization (2019). *The ISO Survey of Management System Standard Certifications 2018*. Dostupno na: https://isotc.iso.org/livelink/livelink?func=ll&objId=20719433&objAction=browse&viewType=1 pristupljeno 04.03.2020.
41. International Organization for Standardization (2020). *About us*. Dostupno na: https://www.iso.org/about-us.html, pristupljeno 04.09.2020.

42. International Organization for Standardization (2020). *ISO Strategy 2016-2020*. Dostupno na: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100364.pdf, pristupljeno 04.09.2020.
43. International Organization for Standardization (ISO) (2018). *Guidelines for auditing management systems* (ISO 19011:2018)
44. International Organization for Standardization (ISO) (2020). *The ISO Survey of Management System Standard Certifications 2018*. Dostupno na: https://isotc.iso.org/livelink/livelink?func=ll&objId=20719433&objAction=browse&viewType=1 , pristupljeno 04.03.2020.
45. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2015). *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements* (ISO/IEC 17021-1)
46. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2019). *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines* (ISO/IEC 27701:2019)
47. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2013). *Information technology — Security techniques — Information security management systems — Requirements* (ISO/IEC 27001:2013)
48. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2013). *Information technology — Security techniques — Code of practice for information security controls* (ISO/IEC 27002:2013)
49. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2018). *Information Technology — Security Techniques — Privacy Framework — Amendment 1: Clarifications* (ISO/IEC 29100:2011/AMD 1:2018)
50. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2011). *Information Technology — Security Techniques — Privacy Framework* (ISO/IEC 29100:2011)
51. International Organization for Standardization (ISO*), ISO/IEC Directives, Part 1, Consolidated ISO Supplement, - Procedures specific to ISO*, Dostupno na:

https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor535, pristupljeno 5.1.2021.

52. OECD (2019), *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, https://doi.org/10.1787/9789264311992-en.
53. Republika Hrvatska, Ministarstvo Uprave, *Prijedlog zakona o provedbi Opće uredbe o zaštiti podataka, s konačnim prijedlogom zakona*. Dostupno na: https://vlada.gov.hr/UserDocsImages//2016/Sjednice/2018/04%20travnja/90%20sjednica%20VRH//90%20-%201.pdf, pristupljeno 07.07.2020.
54. Republika Hrvatska, Ured vijeća za nacionalnu sigurnost (2020). *Informacijska sigurnost – NSA*, Dostupno na: https://www.uvns.hr/hr/ako-je-informacijski-sustav-uskladjen-s-hrn-iso-iec-27001-27002-je-li-uskladjen-i-s-hrvatskim-propisima-informacijske-sigurnosti-o-informacijskim-sustavima, pristupljeno 29.9.2020.
55. Republika Hrvatska, Uredba o mjerama informacijske sigurnosti (NN 46/2008)
56. Republika Hrvatska, Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18)
57. Republika Njemačka, Federalni ured za informacijsku sigurnost (2020). *IT Grundschutz*. Dostupno na: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html, pristupljeno 17.01.2021.
58. UKAS (2020). *Technical Bulletin: ETS ISO/IEC 27701:2019, ISO/IEC 27001 & ISO/IEC 27002*. Dostupno na. https://www.ukas.com/resources/technical-bulletins/technical-bulletin-guidance-on-applying-for-an-extension-to-scope-for-iso-iec-277012019-extension-to-iso-iec-27001-and-iso-iec-27002-for-privacy-information-management/, pristupljeno 17.01.2021.
59. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)
60. Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća Tekst značajan za EGP, dostupno na: https://eur-lex.europa.eu/legal-

content/HR/TXT/?qid=1414068508676&uri=CELEX:32012R1025#ntr3-L_2012316HR.01001201-E0003, pristupljeno 23.10.2019.

61. Vijeće Europe, Europska komisija za učinkovitost pravosuđa (CEPEJ) (2020). *European Possible introduction of a mechanism for certifying artificial intelligence tools and services in the sphere of justice and the judiciary: Feasibility Study*, Pristupljeno 16.12.2020., dostupno na: https://rm.coe.int/feasability-study-en-cepej-2020-15/1680a0adf4
62. Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18), dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html, pristupljeno 11.8.2020.

Sažetak

MODEL UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U USKLAĐIVANJU S EUROPSKOM PRAVNOM REGULATIVOM ZAŠTITE PODATAKA

Europsko je Jedinstveno digitalno tržište (DSM), zahvaljujući e-trgovini i e-upravi, jedan od najvažnijih pokretača europskog gospodarstva. Zbog značajnih promjena uslijed novih načina poslovanja u okolnostima digitalne ekonomije donesen je regulatorni okvir koji ne ovisi o državnim granicama i usmjeren je ka zaštiti privatnosti te informacijskoj sigurnosti. Europski regulativa vezana uz zaštitu osobnih podataka ne nudi procesno primjenjiv način usklađivanja organizacija što je vidljivo u otežanom razumijevanju organizacija oko nužnih prilagodbi organizacijskih, ali i tehničkih aspekata poslovanja. Uz pravne posljedice, neusklađenost s njome dovodi i do značajnih posljedica u smislu otežavanja ili potpune nemogućnosti daljnjeg izvoza na europsko tržište. Ciljevi disertacije su ispunjeni odnosno primarnim istraživanjem je ustanovljena međupovezanost između (1) razumijevanja zahtjeva propisanih Općom uredbom o zaštiti podataka (Uredba EU 2016/679) i (2) nedostatka smjernica za usklađivanje poslovnih procesa s Uredbom te je ustanovljena i orijentiranost plasmanu na europsko tržište. Dobiveni rezultati pokazali su da je većina ispitanika razumjela obveze propisane Uredbom no preko 40 % njih je imalo potrebu za dodatnim stručnim pojašnjenjima, dok gotovo deset posto njih nije uopće razumjelo nove obveze. Nije ustanovljena povezanost između veličine organizacije, kompleksnosti obrade osobnih podataka i percipirane težine usklađivanja s Uredbom, ali su znakoviti indikatori vezani uz izvoz na europsko tržište koji ukazuju da gotovo dvije trećine ispitanika dio svojih prihoda ostvaruje izvozom na EU tržište. U organizacijama u kojima je proces usklađivanja još u tijeku i onima koje tek planiraju pokrenuti proces usklađivanja s Uredbom, čak trećina njih očekuje povećanje udjela prihoda od poslovanja sa zemljama Europske unije u svojim prihodima iako još uvijek nisu ispunile nužan uvjet o usklađivanju s njome. Također, pokazalo se da organizacije koje u svom poslovanju koriste ISO sustave, usklađivanje s Uredbom percipiraju manje teškim te su analizom službenih dokumenata EU-a vezanih uz normizaciju i standardizaciju u uvjetima digitalne transformacije identificirani preferirani ISO u svojstvu zaštite sustava i podataka. Na bazi njihove metodologije napravljen je model koji predstavlja primjenjiv opći okvir za strukturirano uspostavljanje, usklađivanje i provođenje revizije usklađenosti organizacijskih i tehničkih mjera s Uredbom i nacionalnim provedbenim zakonom, ali i ISO/IEC 27001 i ISO/IEC 27701 sustava upravljanja.

Ključne riječi: digitalna ekonomija, informacijska sigurnost i privatnost, zaštita podataka, europska pravna regulativa, europsko jedinstveno digitalno tržište, ISO/IEC 27001, ISO/IEC 27701

Summary

INFORMATION SECURITY MANAGEMENT MODEL IN COMPLIANCE WITH EUROPEAN DATA PROTECTION RULES

Owing to e-commerce and e-government, the European Digital Single Market (DSM) is one of the most important drivers of the European economy. Due to significant changes attributable to ways of doing business in new conditions related to digital economy, a regulatory framework has been adopted that does not depend on state borders and is aimed at protecting information security and privacy. European regulations concerning personal data protection do not offer organizations an applicable process manner of harmonizing with requirements related to organizational and technical measures. Non-compliance with regulations does not only lead to legal but also to other significant consequences, such as aggravated or entirely impossible further exports to the European market. The objectives of the dissertation have been achieved, the primary research has established an intercorrelation between, respectively: (1) the understanding of the requirements prescribed by the General Data Protection Regulation (EU Regulation 2016/679) (2) the nonexistence of guidelines for harmonizing business processes with the Regulation and (3) the orientation to the European market. The obtained results indicated that the majority of respondents understood the obligations set out by the Regulation, but more than 40% of respondents required additional expert clarifications, while almost 10% of them did not understand the new obligations. Moreover, it has been revealed that organizations that apply ISO systems in their business perceive harmonizing with the Regulation as less difficult, and those that use ISO/IEC 27001, in larger amount consider it helpful in meeting the requirements specified by the Regulation. No correlation has been established between the size of the organization, the complexity of personal data processing and the perceived difficulty of harmonizing with the Regulation but significant are the indicators where almost two thirds of respondents is achieving some revenue from the exports to EU market. At the same time, almost one third of respondents believe that their organizations will increase the share of the operating revenue with EU countries in the current year, although they have not yet harmonized their business with the Regulation to the fullest extent. Moreover, it has been revealed that organizations that apply ISO systems in their business perceive harmonizing with the Regulation as less difficult and consequently, the official EU documents regarding standardisation and harmonisation in the conditions of digital transformation have been analyzed as well as preffered ISO standards of information security and privacy for the purpose of system and data protection identified. Based on their methodology, a model has been developed to represent an applicable general framework for the structured establishment, harmonization and compliance audit of organizational and technical measures with the Regulation and the national Act on the implementation of Regulation and/or controls of the ISO/IEC 27001 and ISO/IEC 27701 management system.

Keywords: digital economy, information security and privacy, data protection, European legislation, Digital Single Market, ISO/IEC 27001, ISO/IEC 27701

Popis grafikona, slika i tablica

Grafikoni

Slike

Tablice

Prilog 1.

Upitnik - Model upravljanja informacijskom sigurnošću

Postoje 23 pitanja u upitniku.

Znanstveno istraživanje vezano uz doktorsku disertaciju „Model upravljanja informacijskom sigurnošću u usklađivanju s europskom pravnom regulativom zaštite podataka“

Kontakt za više informacija
Natalija Parlov Una, doktorandica
{[una @ apicura.hr]}

Jeste li Vi osobno uključeni u pitanja o zaštiti osobnih podataka i usklađivanju Vaše organizacije s Općom uredbom o zaštiti podataka?

Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Da, kao odgovorna osoba
- Da, kao dio tima ili projekta
- Ne znam ništa o tome

Koliko stalno zaposlenih ima Vaša organizacija? Molim Vas upišite broj, a ako ne znate točan broj procijenite.

U ovo polje mogu biti upisani samo brojevi.
Molimo unesite svoj odgovor ovdje:

U kojem sektoru djeluje Vaša organizacija? *

Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Privatni sektor
- Javni sektor

Možete li procijeniti koliki se dio prihoda vaše tvrtke odnosi na poslovanje sa zemljama Europske unije odnosno izvoz? Upišite postotak, bez decimala i znaka postotka, npr 25.

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Privatni sektor' at question '3 [P0A]' (U kojem sektoru djeluje Vaša organizacija?)
U ovo polje mogu biti upisani samo brojevi.
Molimo unesite svoj odgovor ovdje:

Smatrate li da će se u ovoj godini taj postotak povećati, ostati isti ili smanjiti?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Privatni sektor' at question '3 [P0A]' (U kojem sektoru djeluje Vaša organizacija?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Povećati se
- Ostati isti
- Smanjiti se

U koje sve svrhe koristite osobne podatke koje prikupljate? Odaberite sve što radite

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Privatni sektor' at question '3 [P0A]' (U kojem sektoru djeluje Vaša organizacija?)
Možete izabrati više odgovora
Molim izaberite **sve opcije** koje vam odgovaraju.

- Primarna svrha (Ugovori, dostava računa i slično)
- Vlastite promotivne kampanje
- Komunikacija nakon kupnje (telefonski, e-mailom)
- Slanje *newslettera* i/ilii tiskanih materijala
- Dijeljenje podataka s trećom stranom (zajednički projekti, podizvođač, naplata i slično)-

Na koje sve načine prikupljate osobne podatke? Odaberite sve što radite

Možete izabrati više odgovora
Molim izaberite **sve opcije** koje vam odgovaraju.

- Na prodajnom mjestu
- Na sajmovima, tijekom promotivnih aktivnosti na terenu
- Putem prijave na mrežnim stranicama i aplikacijama

- Prilikom potpisivanja ugovora
- Putem novčanih transakcija
- Tijekom telefonskog razgovora
- Preko agencija i ostalih trećih strana
- Anketiranjem

Koje sve osobne podatke prikupljate, obrađujete i arhivirate?

UPUTA: Za svaki osobni podatak označite što sve radite, možete označiti više odgovora u retku.

	Prikupljate	Obrađujete	Arhivirate
Ime i prezime			
Broj telefona / mobitela / E-mail adresa			
Fizička adresa			
Medicinski podatci			
Podatci djece			
Snimke video nadzora			

Koliko dugo čuvate prikupljene osobne podatke za koje Vam postojeći regulatorni okvir ne propisuje rok čuvanja?

Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Manje od mjesec dana
- Mjesec do tri mjeseca
- Tri do šest mjeseci
- Šest mjeseci do godinu dana
- Više od godine dana
- Nemamo definiran rok čuvanja podataka

Koje sve načine zaštite informacijskog sustava koristite unutar Vaše organizacije?

Možete izabrati više odgovora
Molim izaberite **sve opcije** koje vam odgovaraju.

- Fizička zaštita okoline (postavljanje lokota, alarma, nadzornih kamera, zaštitar)
- Odlaganje, čuvanje i uništavanje prijenosnih medija s informacijama na siguran način
- Zaštita poslužitelja/servera i računala (kontrola pristupa opremi, zaključavanje uređaja, instalacija sustava za praćenje u slučaju otuđenja opreme, lozinke, identifikacija korisnika preko otiska prsta, prepoznavanja glasa i slično)
- Uvođenje pravila za kreiranje i vijek trajanja lozinki
- Edukacija zaposlenika
- Kontrola pristupa korisničkim programima uvođenjem razine ovlasti
- Kriptiranje podataka
- Korištenje *antispyware* programa
- Korištenje antivirusnih programa
- Korištenje vatrozida (*Firewall* program)
- Angažmanom tima zaduženog za informacijsku sigurnost

Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka? *

Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Da, u potpunosti smo uskladili
- Proces usklađivanja je u tijeku
- Planiramo usklađivanje s Općom uredbom o zaštiti podataka
- Moj pravni subjekt nije obveznik usklađivanja sa Općom uredbom o zaštiti podataka
- Ne znam što je Opća uredba o zaštiti podataka

Jeste li razumjeli nove obveze organizacija propisane Općom uredbom o zaštiti podataka?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Da, u potpunosti smo uskladili ' *ili* 'Proces usklađivanja je u tijeku' *ili* 'Planiramo usklađivanje s Općom uredbom o zaštiti podataka' at question '11 [P7]' (Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Uglavnom niste razumjeli
- Dijelom ste razumjeli ali trebate dodatna pojašnjenja pravnika/ stručnjaka za to područje
- Razumjeli ste u potpunosti

Na koji način planirate uskladiti ili ste usklađivali svoje poslovanje s Općom uredbom o zaštiti podataka? *

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Da, u potpunosti smo uskladili ' *ili* 'Proces usklađivanja je u tijeku' *ili* 'Planiramo usklađivanje s Općom uredbom o zaštiti podataka' at question '11 [P7]' (Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Potpuno samostalno
- Uz manju pomoć vanjskih konzultanata
- Uz veću pomoć vanjskih konzultanata

Ako ste koristili vanjske konzultante, koliko ste zadovoljni provedenom analizom procesa prikupljanja i protoka osobnih podataka unutar Vaše organizacije?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
(((! is_empty(P7.NAOK) && (P7.NAOK == 1)) or (! is_empty(P7.NAOK) && (P7.NAOK == 2))) and ((! is_empty(P9.NAOK) && (P9.NAOK == 2)) or (! is_empty(P9.NAOK) && (P9.NAOK == 3))))
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- 1– uopće niste zadovoljni
- 2
- 3
- 4
- 5– izrazito ste zadovoljni

Koliko ste zadovoljni njihovim poznavanjem pravne regulative vezane uz vaš sektor poslovanja?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Da, u potpunosti smo uskladili ' *ili* 'Proces usklađivanja je u tijeku' at question '11 [P7]' (Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?) *i* Answer was 'Uz manju pomoć vanjskih konzultanata' *ili* 'Uz veću pomoć vanjskih konzultanata' at question '13 [P9]' (Na koji način planirate uskladiti ili ste usklađivali svoje poslovanje s Općom uredbom o zaštiti podataka?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- 1– uopće niste zadovoljni
- 2
- 3
- 4
- 5– izrazito ste zadovoljni

Tko je u Vašoj organizaciji zadužen za Opću uredbu o zaštiti podataka?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Da, u potpunosti smo uskladili ' *ili* 'Proces usklađivanja je u tijeku' *ili* 'Planiramo usklađivanje s Općom uredbom o zaštiti podataka' at question '11 [P7]' (Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?)
Možete izabrati više odgovora
Molim izaberite **sve opcije** koje vam odgovaraju.

- Administrativno osoblje
- Knjigovođa
- Pravnik
- Direktor
- IT stručnjak
- Netko drugi
- Nismo nikoga zadužili za Opću uredbu o zaštiti podataka

Koliko vremena je trajalo usklađivanje vašeg poslovanja s Općom uredbom o zaštiti podataka?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Da, u potpunosti smo uskladili ' *ili* 'Proces usklađivanja je u tijeku' at question '11 [P7]' (Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- manje od tjedan dana
- manje od mjesec dana
- jedan do tri mjeseca
- više od tri mjeseca
- još nismo uskladili poslovanje s Općom uredbom o zaštiti podataka

Proces uvođenja Opće uredbe o zaštiti podataka u Vašu organizaciju biste opisali kao ...

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Proces usklađivanja je u tijeku' *ili* 'Da, u potpunosti smo uskladili ' *ili* 'Planiramo usklađivanje s Općom uredbom o zaštiti podataka' at question '11 [P7]' (Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Izuzetno težak
- Uglavnom težak
- Osrednje težak

- Uglavnom lagan
- Izuzetno lagan

Koliko često pratite preporuke i mišljenja vezana uz provedbu Opće uredbe o zaštiti podataka koje javno objavljuje Agencija za zaštitu osobnih podataka (AZOP) na svojoj internetskoj stranici?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was 'Da, u potpunosti smo uskladili ' *ili* 'Proces usklađivanja je u tijeku' *ili* 'Planiramo usklađivanje s Općom uredbom o zaštiti podataka' at question '11 [P7]' (Jeste li ste uskladili svoje poslovanje s Općom uredbom o zaštiti podataka?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Jednom mjesečno ili češće
- Nekoliko puta godišnje
- Jednom godišnje ili rjeđe
- Nikada

Koje sve ISO sustave upravljanja imate u svojoj organizaciji? *

Možete izabrati više odgovora
Molim izaberite **sve opcije** koje vam odgovaraju.

- nemamo ISO sustave upravljanja
- ISO 9001
- ISO 14001
- ISO 27001
- ISO 50001
- ISO 45001

Koliko vam ISO sustav/i koji imate pomaže/u u organizaciji poslovanja?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was at question '20 [P17]' (Koje sve ISO sustave upravljanja imate u svojoj organizaciji?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Puno pomaže/u

- Donekle pomaže/u
- Ne pomaže/u

Koliko vam ISO 27001 pomaže ili vam je pomogao u uvođenju Opće uredbe o zaštiti podataka?

Odgovori samo ako su sljedeći uvjeti zadovoljeni:
Answer was at question '20 [P17]' (Koje sve ISO sustave upravljanja imate u svojoj organizaciji?)
Izaberite jedan od ponuđenih odgovora
Molim izaberite **samo jedan** od ponuđenih odgovora.

- Puno pomaže
- Donekle pomaže
- Ne pomaže

Koje od sljedećih ISO standarda biste uveli u svoje poslovanje kad biste imali mogućnost?

Možete izabrati više odgovora
Molim izaberite **sve opcije** koje vam odgovaraju.

- niti jedan
- ISO 9001 – Sustavi upravljanja kvalitetom
- ISO 14001 – Sustavi upravljanja okolišem
- ISO 27001 – Sustavi upravljanja informacijskom sigurnošću
- ISO 37001 – Sustavi upravljanja protiv podmićivanja (antikorupcijski)
- ISO 45001 – Zaštita zdravlja i sigurnosti pri radu
- ISO 50001 – Sustavi upravljanja energijom

26.03.2020 – 23:44

Pošalji svoj upitnik.
Zahvaljujemo Vam se na popunjavanju ovog upitnika.

Životopis

Natalija Parlov, doktorandica Međunarodnih odnosa i stručnjakinja za informacijsku sigurnost i bihevioralni marketing. Autorica je brojnih znanstvenih i stručnih radova iz područja informacijske sigurnosti, europske pravne regulative zaštite podataka, bihevioralnog marketinga te plasmana na vanjska tržišta.

Nositeljica je kolegija Digitalna ekonomija na EFFECTUS studiju Financije i pravo, posjeduje psihološko-pedagoško-didaktičko-metodičku naobrazbu i ima izbor u nastavno zvanje predavača.

Certifikacijski je auditor ISO/IEC standarda i sustava upravljanja informacijskom sigurnosti njemačke certifikacijske kuće TÜV NORD te ekspert za usluge digitalnih ključeva (*seals*) i zaštitu osobnih podataka.

Konzultantica je inozemnim i domaćim tvrtkama te institucijama u poljima procesne forenzike i upravljanja rizicima, informacijske sigurnosti, bihevioralne marketinške analitike te usklađivanja javnih i privatnih pravnih subjekata s europskom pravnom regulativom.

Nositeljica je međunarodnih certifikata ISO/IEC 27001 Information Security Management Systems Lead Auditor i ISO/IEC 27701 Privacy Information Management Systems Extension Auditor, ISO 22301 Security and resilience - Business Continuity Management Systems Lead Auditor, ISO 37001 Anti-Bribery Management Systems Lead Auditor, ISO 9001 Quality Management Systems Lead Auditor, te certifikata PMP Project Management Academy, FSB Q-CERT Risk Management, Behavioral Forensic i EU GDPR Privacy DPO Boot Camp & Privacy Level B.

Direktorica je i vlasnica dviju tvrtki – konzultantske tvrtke za standardizaciju procesa, informacijsku sigurnost i usklađivanje s europskom pravnom regulativom zaštite podataka te agencije za digitalni bihevioralni marketing, tržišnu analitiku i plasman na inozemna tržišta.

Kontinuirano surađuje s vodećim domaćim i međunarodnim stručnjacima iz područja forenzike informacijske sigurnosti, tržišne analitike te domaćeg i međunarodnog prava.