UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VPLIV ZAKONODAJNIH SPREMEMB NA INFORMACIJSKI SISTEM – PRIMER IZBRANE ORGANIZACIJE

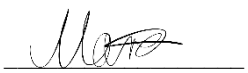
Ljubljana, 17. marec 2026 SEBASTIJAN MAROLT

IZJAVA O AVTORSTVU

Podpisani Sebastijan Marolt, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Vpliv zakonodajnih sprememb na informacijski sistem – primer izbrane organizacije, pripravljenega v sodelovanju z mentorjem red. prof. dr. Petrom Trkmanom

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo pisnih del UL EF, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo pisnih del UL EF;
4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;
7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.
11. da sem preveril verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne 17. 3. 2026 Podpis študenta: 

POVZETEK

Študija primera prikazuje, kako zakonodajne spremembe, kot sta GDPR in IDD, celovito vplivajo na organizacije ter posegajo v vse dimenzije upravljanja storitev. Implementacija zahtev je zahtevala prenovo procesov, prilagoditve informacijskih rešitev, preverjanje skladnosti partnerjev in visoko stopnjo ozaveščenosti zaposlenih. Analiza razkriva, da neenotne časovnice prenosa evropskih zahtev in omejena proaktivnost regulatorjev povečujejo kompleksnost uvajanja skladnosti. V tem kontekstu se ITIL izkaže kot eno ključnih orodij, ki organizacijam omogoča bolj strukturiran, ponovljiv in obvladljiv pristop k uvajanju zakonodajnih sprememb. Uporaba ogrodij ITIL, COBIT in GRC ter sklicevanje na standarde, kot sta ISO 27001 in ISO 29100, pomembno olajšata obvladovanje sprememb. Zakonodajne zahteve se tako izkažejo kot priložnost za izboljšanje procesov, upravljanja podatkov in varnostnih politik.

KLJUČNE BESEDE: GDPR, IDD, ITIL, COBIT, informacijski sistemi, regulativa, digitalna skladnost

CILJI TRAJNOSTNEGA RAZVOJA



ABSTRACT

The case study demonstrates how regulatory changes such as GDPR and IDD have a comprehensive impact on organizations, influencing all dimensions of service management. Implementing these requirements demanded process redesign, adjustments to information systems, verification of partner compliance, and a high level of employee awareness. The analysis shows that inconsistent timelines for transposing EU legislation and limited regulatory proactivity increase the complexity of achieving compliance. In this context, ITIL emerges as one of the key tools that enables organizations to adopt a more structured, repeatable, and manageable approach to implementing regulatory changes. The use of ITIL, COBIT, and GRC frameworks, together with standards such as ISO 27001 and ISO 29100, significantly facilitates the management of change. Regulatory requirements thus become an opportunity to improve processes, data governance, and security practices.

KEY WORDS: GDPR, IDD, ITIL, COBIT, information systems, regulatory framework, digital compliance

SUSTAINABLE DEVELOPMENT GOALS



KAZALO

1 UVOD **1**

2 SKLEPANJE ZAVAROVANJ IN OSEBNI PODATKI V ZAVAROVALNIŠTVU **4**

2.1 Upravljanje z osebnimi podatki **5**

2.2 Opredelitev osebnih podatkov **6**

2.3 Osebni podatki v skladu z zakonom o zavarovalništvu **7**

2.4 Pomen varnosti in zasebnosti posameznika **8**

2.5 Predstavitev zahtev Splošne uredbe EU o varstvu podatkov pri obdelavi osebnih podatkov **9**

2.5.1 Upravljavci/obdelovalci podatkov 11

2.5.2 Vodenje evidence obdelav osebnih podatkov 12

2.5.3 Pravice posameznika, na katerega se nanašajo osebni podatki 13

2.5.4 Tveganja, povezana z osebnimi podatki 15

2.5.5 Vgrajeno in privzeto varstvo podatkov 15

2.6 Predstavitev zahtev direktive o distribuciji zavarovanj **16**

3 MANAGEMENT INFORMATIKE **17**

3.1 Management sprememb **20**

3.2 Management projektov razvoja programske opreme **21**

3.3 Kontrolni cilji za informacijsko tehnologijo in sorodne tehnologije **22**

3.4 Knjižnica infrastrukturnih storitev informacijske tehnologije **24**

3.5 Standardi družine ISO/IEC 27000 ..... **26**

3.6 Zakonodajne spremembe **28**

4 ŠTUDIJA PRIMERA **30**

4.1 Metodologija **30**

4.2 Vpliv Splošne uredbe EU o varstvu podatkov pri obdelavi osebnih podatkov na informacijski sistem izbrane organizacije **31**

4.3 Vpliv Splošne uredbe EU o varstvu podatkov pri obdelavi osebnih podatkov na procese v poslovanju **31**

4.4 Vpeljava podpore za skladnost s Splošno uredbo EU o varstvu podatkov pri obdelavi osebnih podatkov **32**

4.4.1 Vnos privolitev o obdelavi osebnih podatkov 32
4.4.2 Vnos privolitve v ločenem modulu v zalednem sistemu baze strank 33
4.4.3 Vnos privolitve v aplikaciji zalednega sistema za sklepanje zavarovanj 34
4.4.4 Vnos privolitve k obdelavi osebnih podatkov v aplikaciji za zavarovalne zastopnike 35
4.4.5 Vnos privolitve k obdelavi osebnih podatkov v aplikaciji za partnersko mrežo. 35
4.4.6 Beleženje pogledov v osebne podatke strank 36
4.4.7 Anonimizacija podatkov 37
4.4.8 Vodenje zbirk podatkov 37
4.4.9 Dodatna dela za zagotovitev skladnosti s Splošno uredbo EU o varstvo podatkov pri obdelavi osebnih podatkov 38
4.5 Vpeljava podpore za skladnost z direktivo o distribuciji zavarovanj 38
4.5.1 Proces sklepanja zavarovanj pred direktivo o distribuciji zavarovanj in tveganja za stranko 39
4.5.2 Izdaja dokumenta z informacijami o zavarovalnem produktu 39
4.5.3 Test potreb in zahtev in razhajanje s polico 40
5.5.4 Kreiranje police na podlagi izpolnjenega vprašalnika 40
4.5.5 Ostali zahtevani ukrepi za skladnost z direktivo o distribuciji zavarovanj 41
4.6 Povzetek izvedenih sprememb 42
4.7 Ključne ugotovitve študije primera 43
5 SKLEP 46
SEZNAM KLJUČNE LITERATURE 47
LITERATURA IN VIRI 48

KAZALO SLIK

Slika 1: Grafika – Pravne podlage za zasebni sektor, ko obdeluje običajne osebne podatke ... 13
Slika 2: Shema procesa digitalizacije dokumentov 34

SEZNAM KRATIC

angl. – angleško
AZN – Agencija za zavarovalni nadzor
COBIT – (angl. Control Objectives for Information and Related Technologies); Kontrolni cilji za informacijsko tehnologijo in sorodne tehnologije
DPIA – (angl. Data Protection Impact Assessment); Ocena učinka v zvezi z varstvom podatkov
DPO – (angl. Data Protection Officer); pooblaščena oseba za varstvo podatkov
EIOPA – (angl. European Insurance and Occupational Pensions Authority); Evropski organ za zavarovanje in poklicne pokojnine
ENISA – (angl. European Union Agency for Cybersecurity); Agencija Evropske unije za kibernetsko varnost
EU – (angl. European Union); Evropska unija
GDPR – (angl. General Data Protection Regulation); Splošna uredba EU o varstvu podatkov
GRC – (angl. Governance, Risk and Compliance); Upravljanje, tveganja in skladnosti
IDD – (angl. Insurance Distribution Directive); Direktiva o distribuciji zavarovalnih produktov
IDD vprašalnik – (angl. Insurance Distribution Directive Questionaire); IDD vprašalnik
IEC – (angl. International Electrotechnical Commission); Mednarodna elektrotehnična komisija
IPID – Informativni dokument o zavarovalnem produktu (angl. Insurance Product Information Document)
ISACA – (angl. Information Systems Audit and Control Association); Mednarodno združenje za nadzor, revizijo in varnost informacijskih sistemov
ISO – (angl. International Organization for Standardization); Mednarodna organizacija za standardizacijo
IT – (angl. Information Technology); Informacijska tehnologija
ITIL – (angl. Information Technology Infrastructure Library); Knjižnica infrastrukturnih storitev informacijske tehnologije
OGC – (angl. Office of Government Commerce); Britanski urad za vladno trgovino
PESTEL – (angl. Political, Economic, Social, Technological, Environmental and Legal analysis); Analiza političnih, ekonomskih, družbenih, tehnoloških, okoljskih in pravnih dejavnikov
PII – (angl. Personally Identifiable Information); osebni podatki
PIMS – (angl. Privacy Information Management System); sistem upravljanja informacij o zasebnosti
PMP – (angl. Project Management Professional); Mednarodni certifikat za projektne vodje
PRINCE2 – (angl. Projects in Controlled Environments); metodologija vodenja projektov v nadzorovanih okoljih

RegTech – (angl. regulation technology); regulativna tehnologija
RS – Republika Slovenija
SVS – (angl. service value system); sistem vrednosti storitev
ZVOP-1 – Zakon o varstvu osebnih podatkov
ZVOP-2 – Zakon o varstvu osebnih podatkov
ZZavar-1 – Zakon o zavarovalništvu (prenovljena verzija)
ZZavar-1A – Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu, novela A
ZZavar-1B – Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu, novela B
ZZavar-1D – Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu, novela D

1 UVOD

V zadnjih desetletjih so obsežne finančne reforme bistveno preoblikovale delovanje globalnih finančnih trgov. Evropske in nacionalne institucije si s celovitimi zakonodajnimi okviri prizadevajo ponovno vzpostaviti zaupanje trga, okrepiti ključne gospodarske infrastrukture in povečati odpornosti institucij. Številne finančne organizacije se soočajo z velikimi izzivi pri implementaciji novih regulatornih zahtev in z znatnim tveganjem sankcij zaradi morebitnega neskladja z vse bolj kompleksnimi pravili. V nekaterih primerih si ta pravila celo medsebojno nasprotujejo in so predmet lokalnega izvajanja ter sodnih razlag. Takšen primer predstavlja Splošna uredba EU o varstvu podatkov (angl. General Data Protection Regulation, v nadaljevanju GDPR), Uradni list EU, L 119, ki je začela veljati neposredno, vendar je Slovenija morala sprejeti Zakon o varstvu osebnih podatkov (ZVOP-2), Uradni list RS, št. 163/22 in 40/25 – ZInfV-1, da je določila pristojni nadzorni organ in kazenske določbe (Delovna skupina za varstvo podatkov iz člena 29, 2017). Institucije so zaradi neskladnosti ali nezmožnosti izpolnjevanja zakonskih rokov izpostavljene visokim, pogosto večmilijonskim denarnim kaznim (Mohamed in Yildirim, 2021).

Digitalizacija je povzročila, da v sodobnih organizacijah skoraj ni poslovnega področja, ki ne bi bilo informacijsko podprto (Dornberger in drugi, 2018). Informacijski sistemi imajo izrazit vpliv na delovanje organizacij, zato je njihov razvoj odvisen od celostnega pristopa in dobre strategije upravljanja sprememb. Sodobni informacijski sistemi so postali sestavni del vsakdanjega poslovanja in organizacijam omogočajo ohranjanje konkurenčne prednosti (Ćirić in Raković, 2010). Zaradi visoke odvisnosti od informacijskih sistemov je za uspešno izvajanje sprememb nujno dobro sodelovanje med deležniki poslovne in tehnološke strani. Organizacije morajo za ohranjanje konkurenčnosti nenehno usklajevati zahteve zunanjega okolja z notranjimi prilagoditvami. Pri tem ima ključno vlogo strateška usmerjenost k sistematičnemu upravljanju sprememb, ki omogoča strukturirano in konsistentno uvajanje organizacijskih prilagoditev. Učinkovitost tovrstnih procesov je v veliki meri odvisna od sposobnosti organizacije, da spremembe izvaja usklajeno in z optimalno izrabo razpoložljivih virov (Belak, 2010).

Uspešnost vpeljave sprememb je tesno povezana z zmožnostjo vodstva, da učinkovito usmerja in koordinira procese upravljanja sprememb. Pri tem izstopata dve ključni vprašanji: kako se ustrezno pripraviti na implementacijo sprememb in kako obvladati odpor zaposlenih do sprememb (Anderson in Anderson, 2002). Tudi na področju managementa informatike je strateška usmerjenost k prilagajanju, povezovanju in integraciji informacijskih ter poslovnih procesov bistvenega pomena. Prednosti učinkovitega managementa informatike se izrazito pokažejo, ko so informatika in poslovne aktivnosti medsebojno usklajene ter usmerjene k doseganju skupnih organizacijskih ciljev (Ko in Fink, 2010).

Raziskava, ki so jo v zavarovalniški panogi izvedli Sköld in drugi (2020), je pokazala, da regulatornih sprememb ni mogoče enačiti s tehnološkimi spremembami. Avtorji poudarjajo, da je uspešnost implementacije regulatornih sprememb odvisna predvsem od ustreznega upravljanja ključnih virov ter njihovega medsebojnega usklajevanja. Kljub enotnim regulativnim zahtevam za vse udeležence na trgu te spremembe ne ustvarjajo neposredne konkurenčne prednosti za novejše akterje, ki so praviloma tehnološko naprednejši, kar se kaže tudi pri uporabi virov in znanja. Vsi igralci na trgu imajo možnost, da dosežejo uspeh, če znajo učinkovito upravljati svoje komplementarne vire in izkoristiti nove poslovne priložnosti. K razumevanju vpliva regulatornih sprememb na inovacije v finančni industriji dodatno prispeva tudi Freij (2018).

Leta 2018 sta za zavarovalnice stopili v veljavo dve pomembni zakonodajni spremembi – GDPR in direktiva o distribuciji zavarovalnih produktov (angl. Insurance Distribution Directive, v nadaljevanju IDD), ki ju predpisuje Evropska unija (angl. European Union, v nadaljevanju EU). Čeprav sta bili obvezni za vse zavarovalnice, slovenska zakona, in sicer ZVOP-2 ter Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu (ZZavar-1A), Uradni list RS, št. 9/19, do rokov za skladnost (25. maj 2018 in 1. oktober 2018) še nista bila sprejeta. Zavarovalnice so zato morale slediti evropskim zahtevam, hkrati pa so se zavedale tveganja, da skladnost z evropskimi standardi morda ne bo zadostovala za kasnejše zahteve lokalne zakonodaje. Ta situacija je predstavljala pomemben izziv za celotno panogo, saj je zahtevala prilagoditev procesov in informacijskih sistemov. Kljub temu so bile spremembe tudi priložnost za optimizacijo poslovanja ter za izboljšanje varstva osebnih podatkov in pravic strank (Beckett, 2017).

V magistrskem delu obravnavam problematiko ohlapno definiranih zakonodajnih zahtev v kontekstu razvoja informacijskih sistemov v organizaciji. Temo sem izbral zaradi številnih nejasnosti in odprtih vprašanj, s katerimi smo se srečali pri uvajanju informacijske podpore za skladnost z GDPR in IDD. Zaradi zakonsko določenih rokov smo bili izpostavljeni časovnemu pritisku, hkrati pa smo se soočali z izzivi pri načrtovanju razvojnih aktivnosti, saj so se zahteve spreminjale, odgovori na ključna vprašanja pa niso bili enoznačni. Posledično ni bilo mogoče natančno oceniti potrebnega razvojnega napora.

Zagotavljanje skladnosti z zakonodajo predstavlja še posebej velik izziv za organizacije, ki uporabljajo lastno razvite programske rešitve. V takšnih primerih morajo organizacije samostojno identificirati vse zahteve, jih interpretirati in ustrezno implementirati v informacijski sistem, kar zahteva poglobljeno poznavanje zakonodaje ter tesno sodelovanje pravnih in tehničnih strokovnjakov. Organizacije, ki razvijajo lastne informacijske rešitve, morajo zato izvesti temeljito analizo obstoječega stanja, pripraviti načrt prenove, ga potrditi v skladu z notranjimi postopki ter zagotoviti ustrezno informacijsko podporo. Zerlang (2017) opozarja, da

zgolj sledenje dobrim praksam in zakonodaji ni zadostno za učinkovito zagotavljanje kibernetske varnosti v kontekstu digitalne transformacije, saj je nujna vzpostavitev povezav med sistemi in procesi.

Izbrana organizacija se zaradi narave svojega delovanja ukvarja z obsežno obdelavo osebnih podatkov, ki se uporabljajo za različne poslovne namene in predstavljajo ključen del osnovnih delovnih procesov. Osebni podatki se uporabljajo tudi za trženjske aktivnosti in razvoj novih produktov. Pri testiranju programske opreme se organizacija prav tako srečuje z obdelavo osebnih podatkov, saj GDPR šteje vpogled v osebne podatke kot obliko obdelave (Evropska komisija, brez datuma a), zato je nujno, da organizacija dosledno upošteva smernice in zahteve GDPR ter ustrezno ravna z osebnimi podatki, da zagotovi skladnost z zakonodajo in zaščito pravic posameznikov (Informacijski pooblaščenec Republike Slovenije, brez datuma a).

Namen magistrskega dela je raziskati izzive, s katerimi se je organizacija soočala pri vpeljavi informacijske podpore za skladnost z zahtevami GDPR in IDD. Delo temelji na študiji primera iz prakse, ki prikazuje celoten proces implementacije – od analize obstoječih poslovnih procesov in informacijskega sistema do identifikacije potrebnih sprememb, nadgradenj in prilagoditev. S tem magistrsko delo omogoča boljše razumevanje vpliva zakonodajnih zahtev na načrtovanje in izvedbo razvojnih aktivnosti v organizaciji, ki uporablja lastno razvite informacijske rešitve. Tematika je dodatno podprta z domačo in tujo literaturo, ki omogoča umestitev praktičnih ugotovitev v širši teoretični okvir ter prispeva k celovitejši interpretaciji zakonodajnih, organizacijskih in tehnoloških vidikov obravnavanih sprememb.

Cilj magistrskega dela je celovito analizirati vpliv zakonodajnih sprememb GDPR in IDD na informacijski sistem izbrane organizacije ter oceniti, kako te spremembe vplivajo na procese razvoja programske opreme in organizacijskih prilagoditev. Delo želi prikazati, kako zakonodajne zahteve posegajo v arhitekturo informacijskih rešitev, poslovne procese in podporne funkcionalnosti, ter ugotoviti, katere metodologije in okvirji lahko organizaciji pomagajo pri učinkovitem obvladovanju takšnih sprememb. S tem magistrsko delo prispeva k boljšemu razumevanju izzivov, ki nastanejo pri implementaciji regulativ v okolju z lastno razvitimi informacijskimi sistemi.

V splošnem delu predstavim zahteve GDPR in IDD v povezavi s panogo, v kateri organizacija deluje, ter opredelim področje managementa informatike. Nadalje analiziram vpliv obeh zahtev na informacijski sistem organizacije in opišem proces njune vpeljave. V zaključku vzpostavim vzporednice med obema zakonodajnima zahtevama z vidika izzivov pri upravljanju sprememb. Čeprav študija primera temelji na zakonodajnih spremembah iz leta 2018, so spoznanja o upravljanju sprememb relevantna tudi za kasnejše in prihodnje zakonodajne zahteve. Uporaba

starejšega primera omogoča tudi prikaz časovnice prenosa evropskih zahtev v slovenski pravni red.

2 SKLEPANJE ZAVAROVANJ IN OSEBNI PODATKI V ZAVAROVALNIŠTVU

Zavarovalništvo je panoga, ki vpliva na posameznika, gospodarstvo in na družbo kot celoto. Je pomemben mehanizem, ki zagotavlja premoženjsko varnost, finančno in ekonomsko stabilnost (Krumberger, 2015). Prve primitivne oblike zavarovanja so se pojavile s pojavom zasebne lastnine, ko posameznik ni več mogel nositi posledic neukrotljivih in uničujočih pojavov (Bijelić, 1998).

Zavarovanje je že v preteklosti nudilo varnost in zaščito pred raznovrstnimi nevarnostmi. Razširilo se je kot element trgovine in tako postalo nepogrešljivo. Ima velik socialni in ekonomski pomen. Z razvojem je rasel splošni pomen zavarovalništva, osnovni cilj vzajemnosti in solidarnosti pa je ostal nespremenjen (Lehtonen in Liukko, 2012). Dandanes skoraj ne obstaja več nevarnost, ki je ne bi mogli zavarovati. Taka raznovrstnost zavarovanj pa zahteva ustrezen nadzor in ohranjanje zaupanja v zavarovalniški trg.

Zavarovalniški trg je močno reguliran in nadzorovan. Na podlagi Zakona o zavarovalništvu je bila 1. junija 2000 ustanovljena Agencija za zavarovalni nadzor (v nadaljevanju AZN), ko je Vlada Republike Slovenije imenovala strokovni svet in direktorja Agencije (AZN, brez datuma a). Cilji državne nadzorne ustanove na področju zavarovalništva so zmanjševati in odpravljati nepravilnosti v zavarovanju, varovati interese zavarovalcev ter omogočati delovanje zavarovalnega gospodarstva in njegovega pozitivnega vplivanja na celotno gospodarstvo.

Zavarovalnice so dolga leta uporabljale obsežne birokratske postopke, tradicionalne zavarovalne produkte in ustaljene distribucijske modele, ki so se v zadnjih letih spreminjali razmeroma počasi. Posledično se zavarovalna industrija ni razvijala skladno s pričakovanji potrošnikov, kar se odraža v sorazmerno majhnem deležu sklenjenih zavarovanj preko interneta (Pilič in Agafonova, 2017).

Zakon o zavarovalništvu (ZZavar-1), Uradni list RS, št. 93/15, 9/19, 102/20, 48/23, 78/23 – ZZVZZ-T, 84/24 – odl. US in 77/25, kot zavarovalne posle opredeljuje sklepanje in izvrševanje pogodb o premoženjskem in življenjskem zavarovanju ali pozavarovanju, razen obveznih socialnih zavarovanj (2. člen ZZavar-1). ZZavar-1 določa, da AZN na njegovi podlagi izdaja predpise in izvaja nadzor nad zavarovalnicami, zavarovalnimi zastopniškimi in zavarovalnimi posredniškimi družbami ter zavarovalnimi zastopniki in posredniki (AZN, brez datuma b). ZZavar-1 opredeljuje zavarovalnega zastopnika kot osebo, ki ima dovoljenje Agencije za

zavarovalni nadzor za opravljanje poslov zavarovalnega zastopanja, ki jih opravlja na podlagi pogodbe o zaposlitvi ali drugega odplačnega razmerja (547. člen ZZavar-1).

Sodobni potrošniki pričakujejo, da zavarovalnica razume njihove potrebe, preference in pričakovanja. Čeprav se stranke pogosto predhodno informirajo o želenem produktu, se še vedno pogosto odločijo za obisk v poslovalnici ali za srečanje z zavarovalnim zastopnikom, saj pričakujejo dodatno strokovno pojasnilo, osebno svetovanje in prilagojeno ponudbo glede na njihove okoliščine. Raziskava o ponudbi zavarovanj s pomočjo sodobne tehnologije (Nekrep, 2018) je pokazala, da je trženje zavarovalnih produktov v Sloveniji leta 2018 pretežno temeljilo na tradicionalnih distribucijskih kanalih. Zavarovalnice so namreč kar dve tretjini celotne zavarovalne premije zbrale preko lastne mreže zavarovalnih zastopnikov. Statistični podatki zavarovalnic, ki delujejo na slovenskem trgu, kažejo, da notranji in zunanji zastopniki v segmentu premoženjskih zavarovanj ustvarijo od 60 do 65 % celotne premije, medtem ko je pri življenjskih zavarovanjih ta delež še izrazitejši, saj zastopniške mreže prispevajo več kot 80 % skupne obračunane premije.

2.1 Upravljanje z osebnimi podatki

Varstvo osebnih podatkov je v zadnjih letih pridobilo izjemen pomen, saj razvoj informacijske tehnologije bistveno povečuje možnosti za zlorabe osebnih podatkov. V sodobnem digitalnem okolju posamezniki pogosto nezavedno razkrivajo svoje osebne podatke, kar lahko vodi do resnih in dolgoročnih posledic. Ključni element učinkovitega varstva osebnih podatkov na internetu ostaja predvsem ustrezna osveščenost posameznikov o tveganjih in načinih zaščite (Informacijski pooblaščenec Republike Slovenije, brez datuma b).

Organizacije si prizadevajo vzpostaviti kakovosten in trajen odnos s strankami z osebnim pristopom ter poglobljenim razumevanjem njihovih potreb. Za oblikovanje trdnega odnosa med organizacijo in stranko je bistveno, da je stranka postavljena v središče pozornosti ter da se v interakciji z organizacijo počuti sprejeto in razumljeno. Ker so potrebe strank do določene mere primerljive, organizacije pogosto uporabljajo segmentacijo trga (Miguéis in drugi, 2012). Segmentacija lahko temelji na geografskih, demografskih (npr. starost, spol, zakonski status), psihografskih (npr. življenjski slog, osebnostne značilnosti) ali vedenjskih dejavnikih (npr. nakupni motivi, čas nakupa) (Baker in Hart, 2008).

V zavarovalništvu je uporaba osebnih podatkov neizogibna, saj so ti nujni za sklenitev vsakega zavarovalnega posla. Osebni podatki se pridobijo že ob pripravi zavarovalne police, ključno vlogo pa imajo tudi pri obravnavi škodnih primerov. Zato je izjemno pomembno, da so ti podatki ustrezno shranjeni, zaščiteni pred nepooblaščenimi vpogledi in obdelani v varnem informacijskem okolju.

Do leta 2018 je področje varstva osebnih podatkov v zavarovalnicah urejal ZZavar-1, ki kot krovni zakon določa temeljna pravila delovanja zavarovalniškega sektorja v Republiki Sloveniji. Med drugim ureja tudi pridobivanje, vodenje in uporabo zbirk osebnih podatkov (223. člen ZZavar-1).

GDPR je bila po večletnih pogajanjih sprejeta 27. aprila 2016 in je 25. maja 2018 nadomestila direktivo 95/46/ES iz leta 1995. Predhodna direktiva je predstavljala okvir pravic in dolžnosti posameznikov ter obveznosti podjetij in javnih organov, ki zbirajo in obdelujejo osebne podatke, kot navaja v 9. členu Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 177/20 – ZVOPOKD in 163/22 – ZVOP-2.

Njena implementacija pa je bila prepuščena posameznim državam članicam. To je vodilo do neenotne ravni varstva osebnih podatkov v EU (Custers in drugi, 2018). Ključna prednost nove uredbe je njena neposredna veljavnost in zavezujoča narava za vse države članice, kar krepi pravice posameznikov ter zagotavlja enotno raven varstva osebnih podatkov v EU (1. člen GDPR). Posledično pretok osebnih podatkov med državami članicami ni več omejen zaradi razlik v nacionalnih zakonodajah (Trinkaus in Pahor, 2017).

2.2 Opredelitev osebnih podatkov

GDPR osebni podatek opredeljuje kot katerokoli informacijo v zvezi z določenim ali določljivim živečim posameznikom. Mednje sodijo tudi različne posamezne informacije, ki lahko skupaj privedejo do identifikacije določene osebe, in so predstavljene v nadaljevanju.

GDPR je tehnološko nevtralna in varuje osebne podatke ne glede na to, katera tehnologija se uporablja za njihovo obdelavo. Uporablja se za avtomatizirano in ročno obdelavo. Prav tako ni pomembno, kako se podatki hranijo – v informacijskem sistemu, prek videonadzora ali na papirju. V vseh teh primerih za osebne podatke veljajo zahteve glede varstva, ki so določene v splošni uredbi o varstvu podatkov.

GDPR za zmanjšanje tveganj identifikacije in povečanje zasebnosti osebnih podatkov priporoča uporabo psevdonimizacije osebnih podatkov (5. odstavek 4. člena GDPR). Psevdonimizacija pomeni postopek, pri katerem se najbolj prepoznavna polja v podatkovnem zapisu nadomestijo z enim ali več psevdonimi, tj. umetno ustvarjenimi identifikatorji, s čimer se zmanjša verjetnost neposredne identifikacije posameznika. Ker metode psevdonimizacije niso trajne in je podatke mogoče ponovno povezati s posameznikom, takšni podatki še vedno sodijo v področje uporabe GDPR (Politou in drugi, 2018). Pri presoji določljivosti posameznika je treba zavzeti širok pristop in upoštevati vsa sredstva, ki bi lahko omogočala ponovno identifikacijo, bodisi neposredno bodisi posredno (Bolognini in Bistolfi, 2017).

Osebni podatki, ki so anonimizirani na način, da posameznika ni več mogoče določiti niti neposredno niti posredno, prenehajo veljati za osebne podatke. Ključni pogoj za takšno razvrstitev je, da je anonimizacija izvedena popolnoma, tj. da je postopek dokončen in nereverzibilen, kar pomeni, da ponovna identifikacija posameznika ni več mogoča z nobenimi razumno dostopnimi sredstvi (11. člen GDPR).

2.3 Osebni podatki v skladu z zakonom o zavarovalništvu

Zavarovalnice lahko zbirajo, shranjujejo, posredujejo, uporabljajo ali drugače obdelujejo osebne podatke, opredeljene v 268. členu ZZavar-1A, pri čemer morajo ravnati v skladu z zakonodajo, ki ureja varstvo osebnih podatkov ter zbirke podatkov na področju zavarovalništva. ZZavar-1 določa, da zavarovalnice upravljajo naslednje zbirke osebnih podatkov (224. člen ZZavar-1):

- zbirko podatkov o zavarovalcih in zavarovancih,
- zbirko podatkov o zavarovalnih primerih,
- zbirko podatkov za presojo zavarovalnega kritja in višine odškodnine oziroma zavarovalnine,
- zbirko podatkov o potencialnih zavarovalcih in zavarovancih.

Obdelava osebnih podatkov v navedenih zbirkah je dopustna zgolj v obsegu, ki je ustrezen in nujen za doseganje zakonito določenih namenov obdelave. Podatki iz zbirk o zavarovalcih in zavarovancih, zavarovalnih primerih ter podatki za presojo zavarovalnega kritja in višine odškodnine oziroma zavarovalnine se lahko obdelujejo za namene sklepanja in izvajanja zavarovalnih pogodb, izterjave neporavnanih obveznosti iz zavarovalnih razmerij, reševanja škodnih primerov, uveljavljanja povračilnih zahtevkov ter izvrševanja drugih pravic in obveznosti iz zavarovalnih razmerij (ZZavar-1A). Ti podatki se praviloma pridobivajo neposredno od posameznika, na katerega se nanašajo, lahko pa tudi od drugih oseb, iz zbirk podatkov drugih zavarovalnic ali iz drugih zakonsko določenih evidenc (268. člen ZZavar-1A).

Podatki za zbirko podatkov o potencialnih zavarovalcih in zavarovancih se pridobivajo neposredno od stranke. Uporabljajo se za namene svetovanja, ugotavljanja potreb v okviru pogajanj za sklenitev zavarovalne pogodbe ter ocenjevanja primernosti in ustreznosti zavarovalnih storitev oziroma produktov.

ZZavar-1 določa tudi roke hrambe osebnih podatkov v posameznih zbirkah. Osebni podatki o zavarovalcih in zavarovancih se hranijo deset let po prenehanju zavarovalne pogodbe, osebni podatki v zvezi z zavarovalnimi primeri pa deset let po zaključku obdelave posameznega škodnega primera.

Zavarovalnice lahko pridobivajo podatke tudi iz drugih registrov in evidenc, ki jih je mogoče elektronsko izmenjevati. Pri tem zakon natančno določa namene, za katere se lahko podatki pridobivajo, vrste zbirk, iz katerih se podatki lahko črpajo, ter najdaljši dopustni rok njihove hrambe. Posredovani smejo biti zgolj tisti podatki, ki so nujni za konkretno zavarovalno razmerje. Ob tem mora biti zagotovljena sledljivost obdelave, kar vključuje preverljivost pravne podlage, namena posredovanja, identitete oseb, ki so podatke pridobile, čas pridobitve ter obseg nadaljnje obdelave. Sledljivost mora biti zagotovljena za celotno obdobje, v katerem je mogoče uveljavljati pravno varstvo zaradi nedopustnega posredovanja osebnih podatkov.

Po izteku zakonsko določenih rokov hrambe se osebni podatki izbrišejo, uničijo ali nepovratno anonimizirajo. Dokumentacija se uniči na način, ki onemogoča ponovno vzpostavitev njene vsebine ali nadaljnjo uporabo. Enaki pogoji veljajo tudi za podatke, pridobljene z elektronsko izmenjavo zapisnikov policije o prometnih nesrečah, ki jih na podlagi predhodnega naročila pridobiva in hrani Slovensko zavarovalno združenje.

2.4 Pomen varnosti in zasebnosti posameznika

Mnoge podatke nevede izdajamo sami, med drugim so to tudi podatki o naših navadah, o naši lokaciji, o našem zdravstvenem stanju in tudi o hobijih. Primer: z uporabo zemljevidov posredujemo informacijo o naši lokaciji, pri uporabi aplikacij za zunanje športne aktivnosti pa poleg lokacije običajno izdamo tudi precej o našem zdravstvenem stanju in telesnih aktivnostih (Morey in drugi, 2015). Izsledki raziskave o uporabi osebnih podatkov v mobilnih aplikacijah, ki so jo izvedli na Norveškem Brandtzaeg in drugi (2019), so pokazali, da je deljenje osebnih podatkov odvrnilo polovico anketiranih uporabnikov od prenosa mobilne aplikacije na njihov mobilni telefon. Raziskava je pokazala, da je kar 19 od preiskovanih 21 aplikacij pošiljalo posebne podatke na okvirno 600 različnih domen, nekatere aplikacije pa so osebne podatke zbirale in posredovale tudi, ko aplikacija ni bila v uporabi. Čeprav večino uporabnikov skrbi za varnost njihovih osebnih podatkov, pa so o varnosti osebnih podatkov precej nepoučeni, kar s pridom uporabljajo organizacije. Povprečen uporabnik spleta in pametnih naprav se oddajanja teh informacij niti ne zaveda ali pa se mu ta vidik ne zdi pomemben in se brez pomisleka strinja s pogoji uporabe storitve, aplikacije ali spletne strani. Raziskava, ki si sta jo opravila Soumelidou in Tsohou (2021), potrjuje, da se uporabniki kljub zavedanju problematike varovanja zasebnosti postavijo v pasivno vlogo in ne poskrbijo za njeno varovanje. Nasprotno pa je raziskava Mani in Chouk (2019) pokazala, da nepooblaščena sekundarna raba osebnih podatkov in povečani vdori v zbirke osebnih podatkov prispevajo k odporu potrošnikov do uporabe pametnih storitev.

Poleg podatkov, ki jih sami nevede oddajamo ponudnikom, pa nas spremljajo še sistemi, na katere nimamo vpliva, kot so videonadzorni sistemi, sistemi za biometrično prepoznavanje ob

vstopu v objekte ali vodenje zdravstvene dokumentacije. Tudi nekatera javna mesta so že opremili s tehnologijo prepoznavanja obrazov (Falco, 2019). Varovanje zasebnosti postaja dobrina, ki se je moramo zavedati in jo znati v ključnih trenutkih tudi uporabiti (Informacijski pooblaščenec Republike Slovenije, brez datuma b).

Primer iz zavarovalnice je uporaba telemetričnih podatkov za spremljanje načina vožnje uporabnikov (aplikacija DRAJV – Zavarovalnica Triglav). S pomočjo teh podatkov zavarovalnica ve, kje se njeni uporabniki največ gibajo in kateri uporabniki so varni vozniki. V tujini zavarovalnice ponujajo že zavarovanja, ki imajo ceno oblikovano po razredu tveganja, ki ga stranka predstavlja glede na njen način vožnje (Bian in drugi, 2018). Podobne informacije lahko zavarovalnice pridobijo tudi s podatki o škodnih dogodkih, lokaciji nepremičnine, življenjskem slogu, kar je zavarovalnicam v pomoč pri izračunih za višino premije.

2.5 Predstavitev zahtev Splošne uredbe EU o varstvu podatkov pri obdelavi osebnih podatkov

GDPR opredeljuje varstvo posameznikov pri obdelavi osebnih podatkov kot temeljno pravico. V nadaljevanju navaja, da je po členu 8(1) Listine Evropske unije o temeljnih pravicah in členu 16(1) Pogodbe o delovanju Evropske unije (PDEU) določeno, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj (1. člen GDPR).

Za razumevanje zahtev GDPR sta ključni definicija osebnega podatka in definicija obdelave osebnih podatkov:

- **Osebni podatek** pomeni »katero koli informacijo v zvezi z določenim ali določljivim posameznikom; določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika« (4. člen GDPR).
- **Obdelava** »pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje« (4. člen GDPR).

GDPR v temeljnem izhodišču določa, da je njen namen zaščita temeljnih pravic in svoboščin posameznikov, pri čemer posebno pozornost namenja pravici do varstva osebnih podatkov. V 4. členu dodatno poudarja osrednjo vlogo posameznika in zahteva, da mora biti obdelava

osebnih podatkov zasnovana tako, da primarno služi ljudem (4. člen GDPR). Varstvo osebnih podatkov tako ni usmerjeno v zaščito podatkov kot takih, temveč v zaščito pravic posameznika, na katerega se podatki nanašajo.

Pravica do varstva osebnih podatkov se mora uresničevati tako, da je njen obseg sorazmeren z namenom obdelave in uravnotežen z drugimi legitimnimi interesi družbe, kot so varnost, gospodarski razvoj ali učinkovito izvajanje javnih storitev. Nadzor nad zakonitostjo obdelave osebnih podatkov v Republiki Sloveniji izvaja Informacijski pooblaščenec Republike Slovenije, ki skrbi za preprečevanje in odpravljanje kršitev v skladu z določbami GDPR ter relevantne nacionalne zakonodaje (Informacijski pooblaščenec Republike Slovenije, brez datuma c).

Tikkinen-Piri in drugi (2018) poudarjajo, da so osrednje spremembe, ki jih uvaja GDPR, povezane z razširjeno teritorialno veljavnostjo, saj se uredba uporablja tudi za podjetja zunaj EU, kadar obdelujejo podatke posameznikov v EU. Poleg tega uredba krepi temeljna načela, kot so odgovornost upravljavca (angl. accountability), vgrajena in privzeta zasebnost (angl. privacy by design in privacy by default) ter strožje zahteve glede privolitve. Avtorji izpostavljajo tudi nove obveznosti, ki jih morajo izpolnjevati organizacije, med drugim obvezno poročanje o kršitvah varnosti podatkov, izvajanje ocen učinka na varstvo podatkov (angl. Data Protection Impact Assessment, v nadaljevanju DPIA) ter imenovanje pooblaščene osebe za varstvo podatkov (v nadaljevanju DPO) v primerih, ki jih določa uredba. Te spremembe pomembno vplivajo na organizacije, ki zbirajo in obdelujejo osebne podatke, saj zahtevajo prilagoditev notranjih procesov, tehničnih rešitev in praks upravljanja osebnih podatkov.

Nadalje uredba navaja, da se podatki obdelujejo le za določene, izrecne in zakonite namene ter da se prepreči njihova nadaljnja obdelava, ki ni skladna z nameni zbiranja. Podatki morajo biti točni in ažurni ter ne smejo biti hranjeni dlje, kot je potrebno za izpolnitev namena zbiranja. Zahtevana je skrb za celovitost in dostopnost osebnih podatkov, ki sta temeljna stebra varnosti osebnih podatkov (5. člen GDPR). Načelo odgovornosti pa nalaga dolžnost upravljavcem, da so v vsakem trenutku sposobni izkazati skladnost obdelave z zahtevami uredbe in nacionalne zakonodaje.

Kot navaja Informacijski pooblaščenec Republike Slovenije (brez datuma č), mora za obdelavo obstajati ena od pravnih podlag, ki jih predpisuje člen 6(1) GDPR. Osebni podatki se običajno obdelujejo na podlagi privolitve posameznika ali pogodbe, ki jo posameznik sklene z upravljavcem. Za obdelavo posebnih vrst osebnih podatkov, ki so občutljive narave, veljajo strožji pogoji iz člena 9 GDPR. Za zavarovalnice ta del dodatno ureja ZZavar-1A.

Čeprav GDPR določa, da je privolitev eden izmed dopustnih temeljev za obdelavo osebnih podatkov, predstavlja ta zgolj eno od šestih enakovrednih pravnih podlag, opredeljenih v členu

6 uredbe. Rezultati interne ankete, izvedene v Zavarovalnici, v kateri je 80 % sodelujočih menilo, da obdelava brez privolitve ni dopustna, kažejo na razširjeno napačno razumevanje privolitve kot edine zakonite podlage za obdelavo. Takšno nerazumevanje je še posebej problematično v sektorjih, kjer je obdelava podatkov pretežno vezana na pogodbeno razmerje; pri sklenitvi zavarovanja je pravna podlaga za obdelavo osebnih podatkov namreč pogodba, pri čemer obseg podatkov, nameni obdelave in roki hrambe izhajajo iz Zakona o zavarovalništvu. Ugotovitve ankete tako odražajo kompleksnost uredbe in nezadostno komunikacijo njenih zahtev širši javnosti. Kot opozarjajo Horák in drugi (2019), lahko nerazumevanje pravnih podlag v organizacijah vodi v neupravičen previdnostni odziv in pretiran strah pred obdelavo osebnih podatkov, kar negativno vpliva na učinkovito izvajanje zakonitih poslovnih procesov.

Skladnost z GDPR ne pomeni, da je obdelava osebnih podatkov brez privolitve posameznika nedopustna. Ključno je pravilno določiti ustrezno pravno podlago obdelave, saj to omogoča tudi pravilno obravnavo zahtevkov posameznikov, kot so pravica do dostopa, popravka, izbrisa ali ugovora. V zavarovalni praksi je na primer izbris vseh podatkov o zavarovancu nedopusten, kadar zakon določa obvezno hrambo podatkov ves čas trajanja zavarovalne pogodbe in še deset let po njenem prenehanju. Pravilna identifikacija pravne podlage je zato bistvena za zakonito obdelavo podatkov in za dosledno izpolnjevanje obveznosti upravljavca.

V tem okviru je pomembno poudariti, da se številni postopki obdelave v zavarovalni dejavnosti ne opirajo na privolitev, temveč na druge pravne podlage, ki izhajajo iz zakonskih obveznosti ali zakonitega interesa. Tako mora zavarovalnica v skladu z Zakonom o preprečevanju pranja denarja in financiranju terorizma pred izplačilom po polici življenjskega zavarovanja preveriti, ali je upravičenec politično izpostavljena oseba; v takšnih primerih se osebni podatki obdelujejo zaradi izpolnjevanja zakonske obveznosti, zato privolitev ni potrebna. Prav tako se osebni podatki pogosto obdelujejo na podlagi zakonitega interesa upravljavca, na primer pri izvajanju anket o zadovoljstvu strank ali pri preiskovanju sumov zavarovalniške goljufije. Ti primeri dodatno potrjujejo, da zakonita obdelava osebnih podatkov temelji na različnih pravnih podlagah, ki presegajo zgolj privolitev posameznika.

2.5.1 Upravljavci/obdelovalci podatkov

Upravljavec podatkov določi namene, za katere se obdelujejo osebni podatki, in sredstva za njihovo obdelavo. Zaposleni, ki torej obdelujejo osebne podatke v organizaciji, izpolnjujejo naloge, ki jih organizacija izvaja kot upravljavec podatkov (Evropska komisija, brez datuma b).

Upravljavec tesno sodeluje z DPO pri vodenju ustreznih evidenc, izvedbi ocene učinkov na varstvo osebnih podatkov in sprejemanju ukrepov za zmanjšanje tveganj obdelave. Poleg tega

mora zagotoviti, da so vsi postopki obdelave skladni z zakonodajo ter da so v organizaciji vzpostavljeni mehanizmi za stalno spremljanje skladnosti.

Obdelovalec podatkov je običajno tretja oseba, ki v imenu upravljavca zgolj obdeluje osebne podatke. V primeru skupin podjetij lahko eno od njih deluje kot obdelovalec za drugo podjetje (Evropska komisija, brez datuma b). Dolžnosti, ki jih ima obdelovalec do upravljavca, morajo biti določene v pogodbi ali drugem pravnem aktu. V pogodbi je treba navesti, kaj se zgodi z osebnimi podatki ob morebitni prekinitvi pogodbe. Tipična dejavnost obdelovalcev je zagotavljanje rešitev informacijske tehnologije (v nadaljevanju IT), vključno s shranjevanjem v oblaku. Obdelovalec podatkov lahko prenese del svoje naloge na drugega obdelovalca ali imenuje skupnega obdelovalca samo, če pridobi predhodno pisno dovoljenje od upravljavca podatkov (prav tam).

Organizacija je lahko hkrati upravljavec in obdelovalec podatkov, kadar v različnih postopkih nastopa v različnih vlogah ali pa deluje izključno kot upravljavec oziroma izključno kot obdelovalec. Takšna raznolikost vlog zahteva jasno notranjo ureditev, da se zagotovita skladnost z zakonodajo in pravilno izvajanje obveznosti v vsaki posamezni situaciji.

2.5.2 Vodenje evidence obdelav osebnih podatkov

Nova zahteva uredbe je evidentiranje dejavnosti obdelav osebnih podatkov. Zahteva po evidentiranju se deloma prekriva z obveznostjo vodenja kataloga zbirk osebnih podatkov za upravljavce z več kot 50 zaposlenimi, ki jo je urejal ZVOP-1.

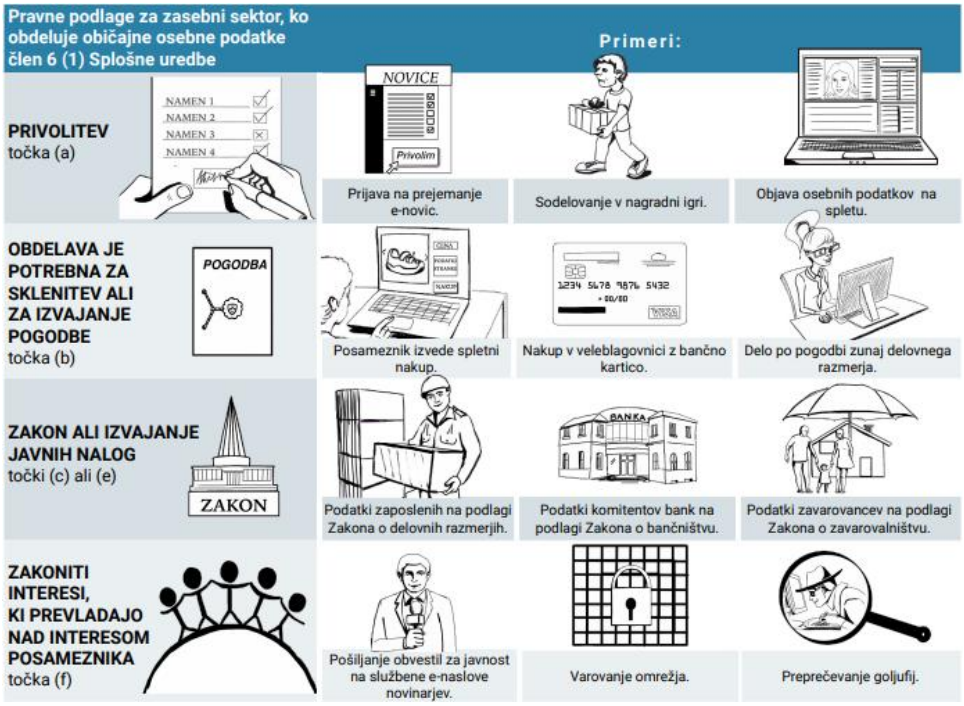
Uredba dodatno nalaga obveznosti tudi za obdelovalce in za vse vrste obdelav osebnih podatkov, ki morajo imeti z začetkom veljave uredbe zagotovljen ustrezen sistem za vodenje evidence dejavnosti obdelav. Večje organizacije morajo po uredbi voditi evidenco glede vseh vrst obdelav osebnih podatkov, kar vključuje: posredovanje podatkov za določen namen, hrambo, izbris itd.

Ugotovitve je treba uporabiti na način, da se komplet dokumentacije, ki opredeljuje področje varstva osebnih podatkov, stalno osvežuje in prilagaja dejanski praksi ter potrebam. Priporoča se, da je beleženje ugotovitev v pisni obliki in ustrezno strukturirano, da omogoča lažje pregledovanje. Pri tem si lahko pomagamo s postopki notranje revizije in drugimi postopki za zagotovitev skladnosti poslovanja, ki lahko pomagajo ugotoviti, katere osebne podatke organizacija obdeluje in kje se nahajajo. Dokumentiranje obdelave osebnih podatkov in ugotovitve, zakaj se obdelujejo osebni podatki, komu se podatki delijo in kako dolgo se hranijo, lahko izvajamo s pomočjo vprašalnikov, pripravljenih za različne dele organizacije, s

pregledovanjem ključnih področij poslovanja (kjer se obdelujejo osebni podatki) in pregledom politik, postopkov, pogodb in dogovorov.

Za namen predstavitve dopustne obdelave osebnih podatkov je Informacijski pooblaščenec Republike Slovenije pripravil grafiko. Ta je prikazana na sliki 1.

Slika 1: Grafika – Pravne podlage za zasebni sektor, ko obdeluje običajne osebne podatke



Vir: Informacijski pooblaščenec Republike Slovenije (brez datuma č).

2.5.3 Pravice posameznika, na katerega se nanašajo osebni podatki

Pomisleki glede varnosti osebnih podatkov na internetu segajo že v prejšnje tisočletje. Tavani (1999) je opozoril, da takrat veljavne smernice in zakonodaja s področja varstva osebnih podatkov niso sledile hitremu tehnološkemu razvoju, zlasti na področju varne rabe interneta in rudarjenja podatkov. Sprejetje GDPR predstavlja pomemben premik v smeri prilagajanja digitalni dobi in novim tehnologijam. Uredba v 15. členu določa, da mora upravljavec posamezniku na njegovo zahtevo potrditi, ali se njegovi osebni podatki obdelujejo, ter mu omogočiti vpogled ali zagotoviti kopijo teh podatkov (Informacijski pooblaščenec Republike Slovenije, brez datuma d).

V razpravah o GDPR je bila pogosto izpostavljena aktivna privolitev posameznika, na kar je opozorila tudi britanska informacijska pooblaščenka Elizabeth Denham (2017). Kljub temu je

privolitev kot pravna podlaga praviloma potrebna predvsem za obdelavo osebnih podatkov v marketinške namene in ne predstavlja temeljnega pogoja za večino obdelav, povezanih z rednim poslovanjem organizacij. GDPR namreč določa šest enakovrednih pravnih podlag za obdelavo osebnih podatkov:

- posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
- obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
- obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
- obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
- obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
- obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

16. člen GDPR ureja pravico do popravka, ki je povezan z načelom točnosti (d) točke 1. odstavka 5. člena GDPR. Posameznik ima pravico zahtevati, da upravljavec brez odlašanja popravi netočne osebne podatke, prav tako pa ima ob upoštevanju namenov obdelave tudi pravico do dopolnitve nepopolnih osebnih podatkov, pri čemer lahko poda dopolnilno izjavo (16. člen GDPR).

Ko navaja 18. člen GDPR ima posameznik pravico, da upravljavec omeji obdelavo, kadar pride do netočnosti podatkov, kadar je obdelava nezakonita oziroma če posameznik vloži ugovor. Pri avtomatiziranih zbirkah mora upravljavec omejitev obdelave zagotoviti s tehničnimi sredstvi na način, da se osebni podatki nadalje več ne obdelujejo in jih ni mogoče spremeniti (18. člen GDPR).

GDPR vključuje več principov zaščite osebnih podatkov, med drugim načelo minimizacije podatkov, omejevanja uporabe in uzakonjenja principov odgovornega ravnanja s podatki, kar izpostavljajo tudi Politou, Michota in drugi (2018). Uredba v 17. členu uvaja pravico do izbrisa, pogosto imenovano tudi pravica do pozabe. Kadar posameznik zahteva izbris osebnih podatkov, mora upravljavec ob upoštevanju razpoložljive tehnologije in stroškov izvedbe sprejeti razumne ukrepe za izbris podatkov ter izbris povezav ali kopij teh podatkov (17. člen GDPR).

Posameznik ima skladno z 18. členom GDPR tudi pravico doseči, da upravljavec omeji obdelavo, kadar pride do netočnosti podatkov, kadar je obdelava nezakonita oziroma če posameznik vloži ugovor (18. člen GDPR). GDPR v 22. členu določa, da ima posameznik, na katerega se nanašajo osebni podatki, pravico, da zanj ne velja odločitev, ki temelji izključno na avtomatizirani obdelavi, vključno z oblikovanjem profilov, kadar ima takšna odločitev pravne učinke ali nanj pomembno vpliva. Izjeme do dopustne le, kadar je avtomatska obdelava nujna za sklenitev ali izvajanje pogodbe, kadar jo določa pravo EU ali države članice, ali kadar temelji na izrecni privolitvi posameznika (22. člen GDPR).

2.5.4 Tveganja, povezana z osebnimi podatki

V kontekstu GDPR je »tveganje« opredeljeno kot kombinacija verjetnosti in resnosti morebitnih negativnih posledic, ki jih lahko obdelava osebnih podatkov povzroči za pravice in svoboščine posameznikov. »Obvladovanje tveganj« pa zajema načrtovanje in izvajanje ustreznih tehničnih in organizacijskih ukrepov, s katerimi upravljavec in obdelovalec zmanjšujeta verjetnost nastanka tveganj ali blažita posledice teh tveganj. GDPR namenja posebno pozornost preventivnim ukrepom varstva osebnih podatkov v okviru temeljnega načela odgovornosti (angl. accountability). To načelo zahteva proaktivno, premišljeno in preventivno ravnanje upravljavcev in obdelovalcev, kar poudarja tudi Delovna skupina za varstvo podatkov iz člena 29 v Smernicah glede ocene učinka v zvezi z varstvom podatkov in opredelitve verjetnosti nastanka velikega tveganja (Delovna skupina za varstvo podatkov iz člena 29, 2017).

GDPR opredeljuje DPIA, ki predstavljajo enega ključnih konceptov v okviru načela odgovornosti (3. odstavek 35. člena GDPR). V istem odstavku uredba določa tudi nekatere primere obdelave, v katerih obstaja veliko tveganje za pravice in svoboščine posameznikov. Mednje sodi zlasti avtomatizirana obdelava, vključno z oblikovanjem profilov, ki ima pravne učinke na posameznika (71. uvodna določba GDPR). Veliko tveganje je prisotno tudi pri uporabi novih tehnologij, obsežnih obdelavah občutljivih osebnih podatkov in pri sistematičnem spremljanju javno dostopnih območij.

GDPR upravljavcu nalaga obveznost, da vsakemu uporabniku, ki so mu bili osebni podatki razkriti, sporoči vse popravke ali izbrise osebnih podatkov ali omejitve obdelave, razen če se to izkaže za nemogoče ali vključuje nesorazmeren napor. Če posameznik, na katerega se podatki nanašajo, to zahteva, mora upravljavec o teh uporabnikih njegovih podatkov posameznika tudi ustrezno obvestiti.

2.5.5 Vgrajeno in privzeto varstvo podatkov

Agencija Evropske unije za kibernetsko varnost (v nadaljevanju ENISA) opozarja, da je GDPR v 25. členu uvedla dva koncepta, ki imata pomemben vpliv na zasnovo informacijskih sistemov: vgrajeno varstvo podatkov (angl. data protection by design) in privzeto varovanje podatkov (angl. data protection by default). Koncepta sta medsebojno tesno povezana in predstavljata temeljna mehanizma za zagotavljanje skladnosti z uredbo v celotnem življenjskem ciklu informacijskih rešitev (ENISA, 2018).

Implementacija vgrajenega varstva podatkov pomeni, da je IT sistem zasnovan tako, da zagotavlja zaščito osebnih podatkov že privzeto, brez potrebe uporabnika po dodatnih posegih ali nastavitvah. Takšna sistemska zaščita vključuje tudi omejevanje dostopa do podatkov, kar je skladno z načeli privzetega varovanja podatkov. Privzeto varovanje podatkov je še posebej pomembno v primerih, ko lahko uporabnik sam spreminja nastavitve, ki vplivajo na obdelavo osebnih podatkov. V takšnih primerih mora biti sistem konfiguriran tako, da privzeto zagotavlja najvišjo raven varstva, uporabnik pa mora aktivno podati soglasje za vsako dodatno obdelavo podatkov. Tipičen primer je uporaba podatkov o lokaciji mobilne naprave, kjer mora biti privzeta nastavitev izklop zbiranja lokacijskih podatkov.

Privzeto varovanje podatkov upravljavcu nalaga obveznost izvajanja ustreznih tehničnih in organizacijskih ukrepov, ki zagotavljajo, da se obdelujejo zgolj osebni podatki, ki so nujno potrebni za posamezen namen obdelave. Koncept temelji na načelu namenske rabe podatkov, minimizacije podatkov in omejitve shranjevanja podatkov, ki jih mora upravljavec upoštevati pri definiranju privzetih nastavitev informacijskih sistemov. ENISA pri tem izpostavlja štiri ključne kriterije:

– Kriterij 1: minimalna količina osebnih podatkov.
– Kriterij 2: minimalna obdelava osebnih podatkov.
– Kriterij 3: minimalno obdobje hrambe osebnih podatkov.
– Kriterij 4: minimalni dostopi do osebnih podatkov.

Upoštevanje teh kriterijev zagotavlja, da osebni podatki niso samodejno dostopni brez izrecnega posredovanja posameznika. To je v celoti skladno z zahtevami 25 Splošne uredbe EU o varstvu podatkov … (25. člen GDPR).

2.6 Predstavitev zahtev direktive o distribuciji zavarovanj

IDD je nastala z namenom okrepitve varstva potrošnikov ter zagotavljanja višje ravni transparentnosti in strokovnosti pri prodaji zavarovalnih produktov. Direktiva zaostruje ter sistematično ureja pravila informiranja in svetovanja strankam (Malinowska, 2016). Od

distributerja zavarovanj (v nadaljevanju prodajnik) zahteva pošten in strokoven odnos do strank ter jih varuje pred nakupom zavarovalnih kritij, ki jih ne potrebujejo ali jih ne želijo.

IDD predpisuje standardiziran prodajni proces, v okviru katerega mora prodajnik pred sklepanjem zavarovalne pogodbe stranki predložiti dokument z informacijami o zavarovalnem produktu (angl. Insurance Product Information Document, v nadaljevanju IPID), kjer so na enostaven in pregleden način zapisane vse značilnosti želenega zavarovanja. Vidonja (2016) poudarja, da je namen dokumenta reševanje več izzivov, ki so bili prisotni v praksi: sodelovanje potrošnikov pri razkritjih, težavne primerjave produktov med zavarovalnicami, pričakovanja stranke v primerjavi z izbranim kritjem na polici (npr. izključene škode pri posameznih kritjih) in prevelik poudarek na ceni zavarovalnih produktov.

V okviru prodajnega postopka mora prodajnik stranki predložiti tudi vprašalnik o potrebah in zahtevah (angl. Insurance Distribution Directive Questionaire, v nadaljevanju IDD vprašalnik), s katerim prodajnik in stranka med prodajnim razgovorom opredelita potrebe po posameznih vrstah in podvrstah zavarovanja. IDD vprašalnik vsebuje dva sklopa: potrebo po zavarovanju in zahtevo po zavarovanju. Prvi sklop odraža objektivno potrebo potrošnika po zavarovanju zaradi obstoja določene nevarnosti in potrebe po finančni zaščiti, medtem ko drugi sklop predstavlja izrecno odločitev potrošnika, da želi določeno kritje dejansko skleniti. Vprašalnik tako ščiti tudi zavarovalnico, saj jasno dokumentira primere, ko se stranka kljub izraženi potrebi odloči, da določenega kritja ne bo sklenila.

Obliko in vsebino IPID-a je predpisal Evropski organ za zavarovanje in poklicne pokojnine (angl. European Insurance and Occupational Pensions Authority, v nadaljevanju EIOPA), zahtevane vsebine dokumenta pa so rubrike:

- Kaj je zavarovano? in Kaj lahko dodatno zavarujem?
- Kaj ni zavarovano?
- Ali je kritje omejeno?
- Kje je zavarovanje veljavno?
- Kakšne so moje obveznosti?
- Kdaj in kako plačam?
- Kdaj zavarovanje začne in kdaj neha veljati?
- Kako lahko odstopim od pogodbe?

3 MANAGEMENT INFORMATIKE

Informacijska tehnologija predstavlja enega ključnih elementov sodobnih organizacij (Sallé, 2004). Z vse tesnejšim prepletanjem informatike in poslovnih procesov se je razvilo tudi

področje managementa informatike (angl. IT governance). Osrednji element upravljanja informatike je zagotavljanje usklajenosti med informacijskimi tehnologijami in poslovnimi cilji organizacije, kar poudarjata tudi De Haes in Van Grembergen (2004). Med področja, kjer je takšna usklajenost še posebej pomembna, sodijo zakonodajne spremembe, saj mora informacijska funkcija zagotoviti ustrezno podporo implementaciji zakonsko zahtevanih prilagoditev ter v sodelovanju s poslovnimi enotami poskrbeti za skladnost organizacije z regulativo.

De Haes in Van Grembergen (2004) ugotavljata, da se je koncept upravljanja informatike pojavil razmeroma nenadno in sprožil številne razprave v organizacijah. Mnoge organizacije so začele implementacijo upravljanja informatike z namenom izboljšanja usklajenosti informatike in poslovanja, kar je prispevalo tudi k večji vključenosti višjega vodstva. Pri tem je pomembno razlikovati med upravljanjem informatike in managementom informatike (angl. IT management), saj gre za konceptualno različni, a medsebojno povezani področji.

Management informatike je opredeljen kot proces, ki zagotavlja učinkovito in uspešno uporabo informacijskih tehnologij pri podpori organizacijskim ciljem. V sodobnem digitalnem okolju management informatike presega zgolj tehnično koordinacijo in vključuje tudi razumevanje širših družbenih in organizacijskih implikacij uporabe informacijskih sistemov. Bélanger in Crossler (2011) poudarjata, da digitalna doba prinaša kompleksne izzive na področju informacijske zasebnosti, kar zahteva, da management informatike vključuje tudi ustrezne mehanizme za zaščito osebnih podatkov, upravljanje tveganj ter zagotavljanje zaupanja uporabnikov. Management informatike se tako ukvarja predvsem s selekcijo IT-projektov, določanjem prioritet, razporejanjem virov ter delitvijo odgovornosti med poslovnimi enotami, IT-vodstvom in zunanjimi izvajalci (Wu in drugi, 2015), ob hkratnem upoštevanju naraščajočih zahtev glede varstva informacij in skladnosti.

IT Governance Institute (2003) poudarja, da je management informatike integrirani del upravljanja organizacije, sestavljen iz vodstva, organizacijske strukture in procesov, ki zagotavljajo doseganje strategije in ciljev na področju IT. Kritični dejavnik uspeha organizacijske strukture in procesov je pogosto učinkovita komunikacija skozi vse ravni organizacije, ki temelji na konstruktivnem odnosu, skupnem jeziku in predanosti k reševanju izzivov.

Robinson (2005) dodaja, da je management informatike neločljivo povezano z upravljanjem tveganj (angl. Enterprise Risk Management – ERM) in kot takšno ne sme delovati ločeno od širšega modela upravljanja organizacije. Zaradi naraščajočega števila regulatornih zahtev in standardov upravljanje informatike pridobiva še večji pomen (Pasquini in Galie, 2013). Za podporo povezovanju poslovnih in IT-ciljev so se razvili različni okvirji, dobre prakse in

standardi, med katerimi so najpogosteje uporabljeni kontrolni cilji za informacijsko tehnologijo in sorodne tehnologije (angl. Control Objectives for Information and Related Technologies, v nadaljevanju COBIT), knjižnica infrastrukturnih storitev informacijske tehnologije (angl. Information Technology Infrastructure Library, v nadaljevanju ITIL) in standardi Mednarodne organizacije za standardizacijo (angl. International Standards Organization, v nadaljevanju ISO). Pri tem pa Overby in drugi (2006) opozarjajo, da se organizacije ne smejo zanašati zgolj na dobro povezanost IT-funkcije in poslovanja, temveč mora biti poslovna stran aktivno vključena v pravočasno zaznavanje zakonodajnih sprememb in tržnih zahtev.

Integriran pristop k upravljanju, tveganjem in skladnosti (angl. governance, risk and compliance, v nadaljevanju GRC) se v zadnjih letih v literaturi vse pogosteje pojavlja kot akronim GRC. Posamezni pojmi kratice so že dobro poznani in uveljavljeni, GRC pa z integracijo vseh treh in s holističnim pristopom prispeva dodatno vrednost organizaciji, saj skrbi za strukturiran pristop k usklajevanju poslovnih ciljev ob hkrati učinkovitem obvladovanju tveganj in zagotavljanju skladnosti (Racz in drugi, 2010). Pravilno izvajanje GRC ima številne koristi za organizacije. Nekatere od teh prednosti vključujejo odločanje na podlagi tveganja, organizacijsko učinkovitost, prepoznavnost, preglednost in poslovno agilnost. GRC pripomore tudi k spodbujanju organizacijske strategije, saj zahteva sodelovanje oddelkov notranje revizije, skladnosti, tveganja, pravne službe, financ, informatike in kadrovske službe, skupaj z vodstvom organizacije (Abdullah, 2019).

Managiranje IT-tveganj je pomembna komponenta informacijske varnosti. IT-tveganje predstavlja negativen vpliv, ki bi ga imela morebitna ranljivost, ob upoštevanju verjetnosti in vpliva pojava (Stoneburner in drugi, 2002). Upravljanje tveganja pa je proces prepoznavanja in ocenjevanja tveganja ter sprejemanja ukrepov za zmanjšanje tveganja na sprejemljivo raven. Končni cilj je pomagati organizacijam pri boljšem obvladovanju tveganj, povezanih z IT.

V finančnem sektorju se je razvila tako imenovana regulativna tehnologija (angl. regulation technology, v nadaljevanju RegTech), ki jo je mogoče opredeliti kot nabor aplikacij in tehnološko podprtih inovacij, namenjenih izpolnjevanju regulatornih zahtev, zahtev skladnosti in poročanja, ki jih morajo izvajati regulirane institucije z namenom povečanja učinkovitosti skladnosti v evropskem finančnem prostoru. RegTech rešitve med drugim naslavljajo širok spekter regulativnih področij, kot so varstvo osebnih podatkov, preprečevanje pranja denarja in financiranja terorizma ter poznavanje strank (European Banking Authority, 2021). Anagnostopoulos (2018) poudarja, da RegTech predstavlja ključen odziv na naraščajočo kompleksnost regulativnih okvirov, saj omogoča avtomatizacijo nadzornih procesov, izboljšano upravljanje podatkov in učinkovitejše spremljanje skladnosti, kar pomembno zmanjšuje operativna tveganja tako za banke kot za regulatorje. Razvoj RegTech rešitev je tako pokazal,

da se informacijska tehnologija lahko uporablja za podporo avtomatiziranega ali polavtomatskega regulativnega spremljanja in poročanja o skladnosti (Arner in drugi, 2017).

3.1 Management sprememb

Management sprememb predstavlja proces usmerjanja organizacijskih sprememb, od najzgodnejših faz zasnove in priprave, preko izvajanja in na koncu do uresničitve rešitve. Učinkovita strategija upravljanja je ključnega pomena za uspešno tranzicijo organizacij ter njihovo prilagajanje novim zahtevam in okoliščinam (Miller, 2020).

V sodobnem IT-ju ima management sprememb veliko različnih podob, zato se pogledi na management sprememb pogosto razlikujejo glede na funkcijo, ki jo posameznik opravlja. Projektni vodje management sprememb običajno razumejo kot postopek pridobivanja odobritev za spremembe obsega, časovnice ali proračuna projekta, medtem ko strokovnjaki za infrastrukturo management sprememb dojemajo kot proces odobritve, testiranja in uvedbe nove strojne opreme, oblačnih storitev ali programskih različic. Postopke za pridobitev odobritev in uvajanje sprememb v projekt ali operativno okolje predpisujejo številne metodologije in standardi, med najpogosteje uporabljenimi pa so ITIL, standard ISO 20000, mednarodni certifikat za projektne vodje (angl. Project Management Professional – PMP) in metodologija vodenja projektov v nadzorovanih okoljih (angl. Projects in Controlled Environments – PRINCE2), kot navajajo de la Cámara in drugi (2012).

Povezava med managementom sprememb in projektnim vodenjem je zato neizogibna, saj obe disciplini obravnavata uvajanje novosti v organizacijsko okolje, vendar z različnimi poudarki. Ključna razlika med disciplinama je v tem, da se management sprememb osredotoča na temeljno dinamiko sprememb, medtem ko projektno vodenje daje večji poudarek metodi in tehniki (Lehmann, 2010; Pollack in Algeo, 2014). Pollack in Algeo (2014) ugotavljata, da je projektno vodenje pogosto obravnavano kot operativna dejavnost, medtem ko je management sprememb na splošno obravnavan kot strateška funkcija.

Osrednji cilj managementa sprememb je zagotoviti, da so spremembe ustrezno ovrednotene, razvrščene po pomembnosti, načrtovane, testirane, uvedene in dokumentirane (Cameron in Green, 2019). Prakse upravljanja sprememb so zasnovane tako, da zmanjšujejo število incidentov, izboljšujejo stabilnost sistemov in zagotavljajo skladnost z regulativnimi zahtevami. Phillips in Klein (2022) ugotavljata, da ustrezno zasnovane prakse omogočajo učinkovito in hitro obravnavanje sprememb IT-infrastrukture in programske kode. Sodobni pristopi k upravljanju sprememb razgrajujejo organizacijske silose, povečujejo preglednost, zmanjšujejo ozka grla in znižujejo tveganja. Hiatt (2006) opozarja, da mora vodstvo zagotoviti dovolj virov

glede na obseg in zahtevnost sprememb, kar potrjuje pomembno vlogo managementa sprememb pri uvajanju novih zakonskih zahtev.

V kontekstu uvajanja GDPR Kotter (2012), da projekti razvoja in implementacije informacijskih sistemov zahtevajo celovit, življenjski pristop, saj se številni projekti izjalovijo. Pri tem je ključno poznavanje kriterijev, ki omogočajo presojo, ali je projekt kljub odstopanjem mogoče šteti za delno uspešen.

Vpeljava GDPR je od organizacij zahtevala obsežne spremembe, pri čemer je strukturiran pristop k managementu sprememb ključnega pomena. Proces je lahko posebej zahteven v velikih organizacijah, kjer se pogosto pojavljajo odpor zaposlenih, počasno odločanje in pomanjkanje jasne vizije. Kotter (2012) poudarja, da je za uspeh nujno ustvariti občutek nujnosti, oblikovati široko koalicijo zaposlenih in zagotoviti, da spremembe postanejo del organizacijske kulture. Uvajanje GDPR ne vpliva zgolj na pravno službo, temveč zahteva, da se pomena skladnosti z uredbo zavedajo vsi, ki upravljajo podatke.

Mnogi direktorji informatike so pri pregledu stanja ugotovili, da predhodne metode upravljanja in obdelave podatkov niso bile ustrezne. Številni so mnenja, da se zahtevnost uvedbe GDPR manj nanaša na upravljanje podatkov in bolj na procese managementa sprememb, saj je veliko podjetij moralo spremeniti način ravnanja s podatki o potrošnikih. Najboljši način za izvedbo teh sprememb je strukturirano upravljanje sprememb, pri čemer Black (2014) poudarja, da je GDPR za večino organizacij dodatna procesna obremenitev. Nadalje se avtor sprašuje, koliko organizacij je izkoristilo priložnost, da GDPR obravnavajo kot gonilo sprememb in pregledajo svoj pristop k upravljanju ter njegovo ustreznost za danes in prihodnost.

3.2 Management projektov razvoja programske opreme

Vodenje projektov kot posebna oblika managementa se je razvila iz prakse vodenja velikih vojaških projektov, kjer je bil za management kompleksnih medsebojnih povezav potreben organiziran pristop med velikim številom različnih nalog, ki jih je opravljalo veliko različnih strokovnjakov. V zadnjih desetletjih se je projektno vodenje pojavilo kot pomembna oblika vodenja za reševanje kompleksnosti timskega dela v organizacijah (Jurison, 1999).

Razvoj programske opreme se skoraj v celoti izvaja projektno. Projekti so praviloma kompleksni, njihov razvoj pa poteka v dinamičnem okolju, kjer se tehnologija in pogoji nenehno spreminjajo. Uporabniki pogosto niso povsem prepričani o svojih potrebah, zato se njihove zahteve spreminjajo med projektom. Posledično se panoga razvoja programske opreme pogosto sooča s prekoračitvami stroškov, zamudami, nizko zanesljivostjo dostavljenih rešitev in nezadovoljstvom uporabnikov (Abdel-Hamid in Madnick, 1991).

Vodnik po znanju projektnega vodenja (PMBOK® vodnik, 7. izdaja) opredeljuje projektno vodenje kot vrednostno usmerjeno disciplino, ki temelji na uporabi znanja, veščin, orodij in tehnik za ustvarjanje vrednosti ter doseganje zastavljenih ciljev projekta (Project Management Institute, 2021). PMBOK 7 poudarja načela, domene uspešnosti in prilagodljivost pristopa glede na naravo projekta. Projektno vodenje tako vključuje sprožitev, načrtovanje, izvajanje ter stalno spremljanje in nadzor aktivnosti, potrebnih za izpolnjevanje projektnih zavez, hkrati pa zahteva učinkovito komunikacijo in redno poročanje o napredku ključnim deležnikom.

Projekti razvoja programske opreme se osredotočajo na tehničine vidike, potrebne za dokončanje projekta ali izdelka. Kakovosten razvojni projekt mora slediti temeljnim načelom programskega inženiringa, ki vključujejo analizo zahtev, pripravo funkcionalnih in tehničnih specifikacij, standarde dokumentiranja, testiranje, vzdrževanje, zagotavljanje kakovosti ter upravljanje konfiguracij. V tem okviru imajo jasno, popolno in nedvoumno opredeljene zahteve ključno vlogo, saj predstavljajo temelj za uspešen in pravočasen razvoj funkcionalnosti, kar poudarjajo tudi Cohen in drugi (2010).

V panogi razvoja informacijskih rešitev se je že pred dvema desetletjema uveljavil agilni pristop, ki se je sčasoma razširil tudi na druga področja. Izkazalo se je, da imajo velike organizacije pogosto težave pri prehodu na izključno agilne prakse. V takšnih okoljih se zato pogosto uporablja hibridni model, ki združuje tradicionalni sekvenčni pristop z odločitvenimi točkami – osredotočen na načrtovanje in preverjanje – z agilnim pristopom, ki je osredotočen na odzivnost in prilagodljivost. Ta kombinacija se je izkazala za učinkovito, vendar zahteva jasno usklajenost med projektno ekipo, cilji organizacije in izvedbo projekta (Zasa in drugi, 2020).

Za podporo projektnemu vodenju so na voljo orodja, ki nam pomagajo pri pripravljalnih delih projekta, pri organizaciji nalog in pregledu nad nalogami, kar tudi zmanjša možnosti napačne komunikacije in nesporazumov. Orodja za podporo projektnemu vodenju prispevajo tudi k učinkovitemu upravljanju časa, podpirajo timsko delo, samoupravljanje in odgovornost. Njihove glavne prednosti so: zagotavljanje jasnih ciljev, preglednosti in sinhronost (Varajão in drugi, 2020).

3.3 Kontrolni cilji za informacijsko tehnologijo in sorodne tehnologije

COBIT je leta 1996 razvilo mednarodno združenje za nadzor, revizijo in varnost informacijskih sistemov (angl. Information Systems Audit and Control Association, v nadaljevanju ISACA) kot okvir za vzpostavljanje kontrolnih mehanizmov na področju informacijskih tehnologij. COBIT z opisom dobrih praks nudi pomoč podjetjem pri razvoju, organizaciji in izvajanju strategij upravljanja informacij ter upravljanja IT-procesov. Poslovna naravnanost okvira

COBIT vzpostavlja povezavo med strateškimi cilji in informacijsko infrastrukturo. To dosega z uporabo zrelostnih modelov in metrik za ocenjevanje doseženih rezultatov ter z jasnim določanjem poslovne odgovornosti za izvajanje IT-procesov.

Najnovejša različica okvira, tj. COBIT 2019, je bila izdana novembra 2018 in je nadomestila različico COBIT 5 iz leta 2011. Na najvišji ravni COBIT vzpostavlja tristopenjsko okvirno strukturo za upravljanje informacijske tehnologije, ki vključuje tri ključne segmente:

- **Poslovne zahteve** (merila za informacije), ki zajemajo temeljne dimenzije kakovosti, kot so integriteta, uspešnost, razpoložljivost, učinkovitost, skladnost, zaupnost in zanesljivost.
- **IT-vire**, med katere sodijo infrastruktura, aplikacije, informacije in človeški viri, ki skupaj predstavljajo osnovo za učinkovito izvajanje IT-procesov.
- **Procese v informatiki**, razdeljene na domene procesov, ki omogočajo strukturirano obravnavo, nadzor in optimizacijo izvajanja IT-aktivnosti.

COBIT je široko priznan in usklajen z različnimi mednarodnimi standardi, kot so ITIL, CMMI, TOGAF, PMBOK in ISO 27000, s katerimi se dopolnjuje. Zaradi svoje celovitosti je pogosto obravnavan kot krovni okvir za poenotenje procesov v celotni organizaciji (De Haes in drugi, 2013). COBIT 2019 je posebej primeren za organizacije, ki uporabljajo več različnih okvirov (npr. ITIL, ISO/IEC 20000, CMMI) ali lastne interne standarde, ter za organizacije, ki morajo upoštevati specifične regulativne zahteve državnih ali lokalnih organov (White, 2023).

COBIT 2019 organizacijam pomaga pri prilagajanju obstoječih okvirov v organizaciji in razumevanju, kako se bo vsak okvir ujemal s splošno strategijo. Podjetjem lahko pomaga tudi pri spremljanju uspešnosti teh drugih okvirov, zlasti glede skladnosti z varnostjo, varovanja informacij in obvladovanja tveganj, področje, ki ga obravnava tudi GDPR.

V literaturi je pogosto poudarjeno, da je učinkovito upravljanje IT-okvirov tesno povezano s strateško usklajenostjo informacijske tehnologije in organizacijskimi cilji. Tallon in Pinsonneault (2011) opozarjata, da lahko visoka stopnja IT-usklajenosti deluje kot omogočevalec organizacijske agilnosti, saj podpira hitrejše odločanje in učinkovitejše procese, vendar lahko pretirana standardizacija, ki pogosto spremlja uvedbo obsežnih okvirov, povzroči tudi rigidnost. Njune ugotovitve poudarjajo potrebo po uravnoteženju med nadzorom in fleksibilnostjo, kar je ključno tudi pri implementaciji COBIT, ki mora hkrati zagotavljati stabilnost procesov in omogočati agilno odzivanje na spremembe.

COBIT je zasnovan tako, da višjemu vodstvu omogoča jasnejši vpogled v povezavo med tehnologijo in organizacijskimi cilji. Poslovne izzive oziroma točke bolečine je mogoče neposredno preslikati v posamezne elemente okvira, kar poudarja potrebo po pristopu »IT, ki jo

vodi nadzor«, kot ga opredeljuje ISACA. Okvir direktorjem informatike in drugim vodjem omogoča, da utemeljijo donosnost naložb v informacijske projekte ter pokažejo, kako ti projekti prispevajo k doseganju ključnih poslovnih ciljev.

V peti izdaji je COBIT vključil tudi Val IT, tj. okvir, ki podjetjem pomaga pri izbiri, implementaciji in optimizaciji naložb v IT za ustvarjanje dolgoročne vrednosti. S tem se je okvir razširil v celovito metodologijo, ki poleg upravljanja procesov omogoča tudi sistematično vrednotenje koristi, stroškov in tveganj IT-naložb ter tako podpira bolj utemeljeno strateško odločanje (Lombardi in drugi, 2016).

3.4 Knjižnica infrastrukturnih storitev informacijske tehnologije

ITIL je zbirka priporočil, širše znana kot ITIL, in sestavlja metodologijo za izvajanje dobre prakse upravljanja informacijske tehnologije v podjetju. Prvotna usmeritev ITIL-a je bila upravljanje informacijske infrastrukture v angleških vladnih ustanovah. Danes se ITIL uporablja po vsem svetu in velja za enega izmed pomembnejših standardov v gospodarstvu, za njegov nadaljnji razvoj pa skrbi AXELOS, tj. skupno podjetje med družbo Capita in Britanskim uradom za vladno trgovino (angl. Office of Government Commerce – OGC). Trenutno aktualna izdaja je ITIL 4, ki je izšla februarja 2019 (Agutter, 2020).

Zbirka ITIL ne nudi strogih receptov, temveč priporočila in napotke najboljših praks za celoten življenjski cikel upravljanja IT-storitev (Reiter in Miklosík, 2020). Zaradi svoje zasnove ima metodologija ITIL bistveno prednost pred drugimi podobnimi metodologijami. Razvita je bila tako, da poleg teoretičnih vsebin, ki so osnovane na praktičnih primerih, zajema tudi širok spekter dodatnih, podpornih oziroma dopolnilnih storitev, na podlagi katerih je bilo oblikovano poslovno področje (Krajnc, 2005).

V četrti izdaji uvaja še jasnejše koncepte, kot so ustvarjanje vrednosti in rezultati storitev. Ključna nova komponenta je tako imenovan sistem vrednosti storitev (angl. service value system, v nadaljevanju SVS), ki vključuje principe, najboljše prakse, nadzor in nenehno izboljševanje storitev z namenom dodajanja vrednosti vsem deležnikom (Richter in Lantow, 2022).

SVS navaja pet elementov, ki podpirajo pretvorbo povpraševanja v rezultate:

- **Smernice** – priporočila, ki lahko vodijo organizacijo v vseh okoliščinah, ne glede na spremembe njenih ciljev, strategij, vrste dela ali strukture vodenja.
- **Upravljanje** – sredstva, s katerimi se organizacija usmerja in nadzoruje.

- **Veriga vrednosti storitve** – nabor medsebojno povezanih dejavnosti, ki jih organizacija izvaja, da bi svojim strankam zagotovila dragocen izdelek ali storitev in olajšala uresničevanje dodane vrednosti.
- **Prakse** – nabor organizacijskih virov, namenjenih opravljanju dela ali doseganju cilja.
- **Nenehno izboljševanje** – ponavljajoča se organizacijska dejavnost, ki se izvaja na vseh ravneh, z namenom stalnega zagotavljanja uspešnosti organizacije po pričakovanju deležnikov.

Za dosego ciljev je ključno, da organizacije celovito pristopijo k načinu konceptualizacije, razvoja in upravljanja storitev. Za ta namen in v pomoč doseganju želenih ciljev ITIL 4 uvaja štiri dimenzije upravljanja storitev, ki so skupaj ključne za učinkovito in uspešno zagotavljanje vrednosti strankam in drugim deležnikom (Reiter in Miklosík, 2020).

Te dimenzije so (Agutter, 2020):

- **Organizacije in ljudje** – poudarja pomen ljudi, njihovih veščin, kompetenc in kulture. Jasno opredeljene vloge, odgovornosti ter odprta komunikacija so nujni za uspešno vodenje in izvajanje storitev.
- **Informacije in tehnologija** – osredotoča se na podatke, informacijske sisteme in tehnološke rešitve, ki podpirajo zasnovo, dostavo in izboljševanje storitev. Poudarja pomen zanesljivosti, varnosti in pravočasnosti informacij v informacijskih sistemih, od katerih postajajo organizacije vse bolj odvisne.
- **Partnerji in dobavitelji** – obravnava odnose, pogodbe in modele sodelovanja, ki prispevajo k ustvarjanju vrednosti ter zmanjševanju tveganj v dobavni verigi.
- **Vrednostni tokovi in procesi** – ukvarja se z integracijo in usklajenostjo delov organizacije za dosego ciljev. Opredeljuje tok vrednosti kot zaporedje korakov, s katerimi organizacija ustvarja in dostavlja storitve ter izdelke.

Iden in Eikebrokk (2013) v svoji sistematični pregledni študiji poudarjata, da uspešna implementacija upravljanja IT-storitev zahteva celovit in uravnotežen pristop k različnim organizacijskim dimenzijam, saj lahko zanemarjanje katere koli od njih pomembno omeji vrednost, ki jo organizacija ustvarja za svoje deležnike. Poleg notranjih organizacijskih dejavnikov pa morajo organizacije pri upravljanju storitev upoštevati tudi širše zunanje vplive, ki jih literatura pogosto obravnava skozi okvir analize političnih, ekonomskih, družbenih, tehnoloških, okoljskih in pravnih dejavnikov (angl. Political, Economic, Social, Technological, Environmental and Legal analysis – PESTEL). Na pomen razumevanja teh zunanjih dejavnikov opozarjata tudi Karadzhov in Patarchanova (2025), ki izpostavljata, da lahko spremembe v političnem, ekonomskem in tehnološkem okolju bistveno preoblikujejo stabilnost in zrelost storitvenih ekosistemov.

Na posamezne dimenzije vpliva šest ključnih zunanjih dejavnikov, ki jih je treba upoštevati z vidika obvladovanja tveganj (Karadzhov in Patarchanova, 2025):

- **Politično** – spremembe vodstva v organizaciji ali širšem političnem okolju lahko vplivajo na podporo storitvam ali praksam upravljanja.
- **Ekonomsko** – nihanja obrestnih mer, cen energentov ali stroškov dela lahko vplivajo na stroškovno učinkovitost in vzdržnost storitev.
- **Družbeno** – preference in pričakovanja uporabnikov se spreminjajo, pri čemer raznolikost deležnikov otežuje oblikovanje enotnega pristopa k upravljanju storitev.
- **Tehnološko** – razvoj tehnologij, kot so umetna inteligenca, obdelava velikih podatkov, kriptovalute ali avtomatizirana dostava, bistveno vpliva na zasnovo in izvajanje storitev.
- **Pravno** – regulative, kot je GDPR, uvajajo strožje zahteve glede ravnanja z osebnimi podatki in zasebnostjo uporabnikov.
- **Okoljsko** – podnebne spremembe in trajnostna pričakovanja potrošnikov vplivajo na to, kako organizacije oblikujejo in izvajajo svoje storitve, saj kupci vse pogosteje preferirajo okoljsko odgovorne ponudnike.

3.5 Standardi družine ISO/IEC 27000

ISO je skupaj z Mednarodno komisijo za elektrotehniko (angl. International Electrotechnical Commission, v nadaljevanju IEC) izdala nabor standardov ISO/IEC 270xx, ki določa pravila in smernice pri sistemu upravljanja varovanja informacij (v nadaljevanju SUVI). Implementacija standardov družine ISO/IEC 270xx organizacijam nudi okvir in smernice za upravljanje varnosti informacij, vključno s finančnimi podatki, osebnimi podatki, intelektualno lastnino, podatki o zaposlenih in o informacijah, ki jim jih zaupajo stranke ali tretje osebe (ISO, 2018). V letu 2018 je februarja izšla tudi nova izdaja standardov omenjene družine, in sicer ISO/IEC 27000:2018, ki v obzir vzame tudi GDPR. Nova izdaja je namenjena vsem tipom in velikostim organizacij, ponuja nam razumevanje o medsebojnem odnosu, obsegu, vlogah in funkcijah vseh standardov v družini (ISO, 2018).

ISO/IEC 27001 je med najbolj prepoznavnimi standardi na področju varovanja informacij, ki zagotavlja zahteve za sistem upravljanja informacijske varnosti. Področje uporabe mednarodnega standarda za SUVI temelji na vzpostavitvi, vzdrževanju, izvajanju in nenehnem izboljševanju SUVI v okviru organizacije, ki bo standard implementirala. Standard je oblikovan tako, da ustreza vsem vrstam organizacij, ne glede na njihovo velikost ali naravo poslovanja. Zapisan je v obliki zahtev in obsega deset poglavij oz. poglavij in prilogo A, v kateri so opredeljeni cilji kontrol in varnostne kontrole. Za zagotovitev skladnosti mora organizacija v celoti upoštevati vse zahteve v točkah od 4 do 10. Te urejajo predvsem področja, ki se nanašajo na organiziranje sistema upravljanja varovanja informacij. V prilogi A je skozi 11 poglavij

navedenih 114 kontrol iz standarda ISO/IEC 27002, za katere je treba za vsako neupoštevano kontrolo navesti razlog opustitve (ISO, 2013).

ISO/IEC 27002 podaja smernice za zagotavljanje informacijske varnosti v organizacijah. V štirinajstih poglavjih je opisanih 114 kontrol, ki so namenjene doseganju 35 različnih ciljev. Standard je bil sprejet z namenom, da organizacijam pomaga pri vzpostavitvi kontrol pri upravljanju informacijske varnosti in ponuja nabor možnih ukrepov za nadzor prepoznanih tveganj, ki so se z leti uporabe v različnih organizacijah po svetu pokazali kot primeri dobre prakse (ISO, 2013).
ISO/IEC 27005 je namenjen upravljanju tveganj informacijske varnosti. Oblikovan je v podporo standardoma ISO/IEC 27001 in ISO/IEC 27002. Standard vsebuje smernice za ocenjevanje in vrednotenje tveganj, implementacijo ustreznih nadzorstev, nadzorovanje in pregledovanje tveganj kot stalen ali periodičen proces in vzdrževanje ter stalno izboljševanje sistema nadzorstev. Z upravljanjem tveganj se predvidijo scenariji in možne posledice ter določijo ukrepi, s katerimi se zmanjša tveganje na sprejemljivo raven (ISO, 2011a).

ISO/IEC 27018 razširja zahteve standardov ISO/IEC 27001 in ISO/IEC 27002, njegov namen pa je predstaviti kontrole, cilje in smernice za implementacijo ukrepov za zavarovanje osebno določljivih podatkov (angl. personal identifiable information, v nadaljevanju PII) v povezavi z načeli zasebnosti standarda ISO/IEC 29100 za okolje javnih oblačnih storitev (ISO, 2019a).

ISO/IEC 27701:2019 je bil predstavljen v avgustu 2019 kot standard za upravljanje osebnih podatkov. Standard določa zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja varovanja osebnih podatkov (angl. privacy information management system, v nadaljevanju PIMS). Ustvarjen je bil kot razširitev standarda ISO/IEC 27001 in ISO/IEC 27002 za nadzor zasebnosti v kontekstu organizacije. Standard narekuje zahteve v povezavi s PIMS in predstavlja smernice za PII upravljavce in obdelovalce, ki so odgovorni za obdelavo osebnih podatkov (ISO, 2019b). Ob tem je pomembno poudariti, da je danes na voljo že posodobljena izdaja standarda ISO/IEC 27701:2025, ki med ključnimi prednostmi izpostavlja tudi to, da organizacijam pomaga izkazovati skladnost z globalnimi predpisi o zasebnosti, kot je GDPR (ISO, 2025).

ISO 29100 vzpostavlja splošni okvir zasebnosti za varovanje osebnih podatkov v informacijsko-telekomunikacijskih sistemih. Namen standarda je pomagati organizacijam pri razumevanju koncepta zasebnosti z naslednjimi elementi, ki so zajeti v standardu (ISO, 2011b):

- skupna terminologija, ki se navezuje na zasebnost,
- opredelitev subjektov in njihovih vlog pri obdelavi PII,
- opis zahteve varovanja zasebnosti,

– sklici na zakonodajo in že poznane dobre prakse pri konceptu zasebnosti ter splošnih načelih.

3.6 Zakonodajne spremembe

Čeprav posamezniki zakonskih sprememb pogosto ne občutimo neposredno, se morajo organizacije nanje odzvati z ustreznimi prilagoditvami poslovnih procesov in nadgradnjami programske opreme. Obseg potrebnih virov je odvisen predvsem od narave zakonodajnih sprememb in kompleksnosti obstoječe programske opreme. Le z načrtnim pristopom in premišljenim upravljanjem virov lahko organizacije zagotovijo skladnost ter hkrati ohranijo operativno učinkovitost (Freij, 2021).

Zagotavljanje skladnosti z zakonodajo je sicer lahko precej enostavno, kadar imamo opravka s kupljeno programsko opremo, kjer skladnost z zakonodajo običajno zagotovi že ponudnik programske opreme v obliki posodobitev oziroma nadgradenj. V tem primeru je naša odgovornost predvsem, da poskrbimo za pravočasno nadgradnjo sistema (Aubert in drugi, 1999). V študiji primera sem se osredotočil na aktivnosti, ki jih je morala dana organizacija izvesti, ker pri svojem delovanju uporablja lastno razvito programsko opremo.

GDPR velja za vse organizacije in ureja varstvo osebnih podatkov posameznikov v EU. Nasprotno pa je IDD namenjena le zavarovalnicam in varovanju potrošnikov. IDD si prizadeva za večjo preglednost in primerljivost zavarovanj. Pri slovenskem zavarovalnem združenju menijo, da bodo novosti koristile tako zavarovalcem kot zavarovalnicam ter prodajalcem (distributerjem) zavarovanj. Uveljavitev direktive bo okrepila varstvo potrošnikov in zaupanje v zavarovalniški trg. Čeprav bi se organizacija lahko odrekla zbiranju osebnih podatkov za trženjske namene, bi še vedno morala upoštevati IDD, ki predpisuje postopek prodaje zavarovanj v skladu z navodili direktive.

Predlog GDPR je bil podan že januarja 2012, obravnavan pa je bil marca 2014 (European Parliament, brez datuma). Po objavi v Uradnem listu Evropske unije 4. 5. 2016 je GDPR začela veljati že 25. 5. 2016 (Informacijski pooblaščenec Republike Slovenije, brez datuma e), njene določbe pa so se morale neposredno uporabljati v vseh državah članicah v dveh letih, torej do 25. 5. 2018. Rok za prenos določb uredbe v nacionalno zakonodajo je bil prav tako dve leti. V Sloveniji je bil ZVOP-2, ki obravnava varstvo osebnih podatkov, po usklajevanjih, dne 17. 12. 2021, kot predlog predpisa uvrščen v redni zakonodajni postopek in sprejet 15. 12. 2022 (Uradni list Republike Slovenije, 2023). To kaže na očitno zamudo slovenske zakonodaje.

Podobno kot GPDR je Direktiva o distribuciji zavarovanj kot Direktiva (EU) 2016/97 Evropskega parlamenta in sveta stopila v veljavo 22. 2. 2016 (Financial Conduct Authority,

2018). Rok uvedbe je bil do 23. 2. 2018, ki pa je bil kasneje preložen na 1. 10. 2018 (AZN, 2020). IDD je bila v slovensko zakonodajo vpeljana z ZZavar-1A, ki je bil v uradnem listu objavljen 11. 2. 2019.

Prvotni rok za veljavo IDD je bil 23. februar 2018, vendar je 14. februarja 2018 Evropski svet napovedal preložitev roka na 1. november 2018. S tem se je rok za zagotovitev skladnosti z njenimi zahtevami podaljšal za dodatnih sedem mesecev (Hodgson, 2018).

Upoštevanje IDD je bilo torej obvezno od 1. 10. 2018. Običajno se direktive v domači pravni red (torej v veljavo v posamezni državi) prenesejo s sprejemom ustreznega zakona. V Sloveniji Državni zbor do evropskega roka za veljavo ni sprejel potrebnih zakonskih sprememb, konkretno Zakona o zavarovalništvu. Kljub temu so se v zavarovalnice, članice Slovenskega zavarovalnega združenja, odločile, da bodo še pred sprejemom ustreznih sprememb zakona postopoma začele slediti zahtevam direktive (Slovensko zavarovalno združenje, 2018).

IDD v slovenski zakonodaji ureja ZZavar-1, in sicer prvič ZZavar-1A, objavljen 11. 2. 2019, nato pa ga je dopolnil Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu (ZZavar-1B), Uradni list RS, št. 102/20, ki je bil 22. 7. 2020. Zadnja iteracija Zakona o zavarovalništvu je bila v uradnem listu objavljena 7. 10. 2025 kot Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu (ZZavar-1D), Uradni list RS, št. 77/2025.

V obeh primerih je bila zakonska zahteva podana kot predpis Evropske unije, kot je bil podan tudi rok za izvedbo in zagotovitev skladnosti z zahtevama, pri čemer je v primeru GDPR šlo za uredbo, ki je neposredno izvršljiva, pri IDD pa za direktivo, ki sama po sebi zavezuje le cilj, ne pa tudi same izvedbe in le-to prepušča lokalni zakonodaji (Evropska unija, brez datuma). Zakonodajni organi so morali evropske zahteve uzakoniti tudi v lokalni zakonodaji, kar so storili z zamikom. V gospodarstvu je bil prisoten strah, da bodo zahtevani ukrepi v slovenski zakonodaji strožji od tistih v uredbi (Djinović, 2018). Če bi se strah upravičil, bi morali po roku za skladnost z zahtevama (maj 2018 za GDPR in november 2018 za IDD) uvajati dodatne zahteve v že nadgrajen informacijski sistem. Ponovno bi morali predvideti razvojne ure za razvoj in vpeljavo dodatne podpore za skladnost z zakonoma.

Za tržne namene GDPR zahteva, da stranke izrecno dovolijo obdelavo svojih osebnih podatkov (aktivna privolitev). To soglasje ne sme biti pogojeno z uporabo storitev ali nakupom izdelka. Pred GDPR je bila praksa, da so bile ob podpisovanju dokumentov že privzeto označene kljukice za obdelavo osebnih podatkov, ki so se na željo stranke odstranile (privzeta privolitev), ali pa so bile klavzule o obdelavi osebnih podatkov vključene v samo pogodbo. Poleg tega se je zaostrila uporaba osebnih podatkov za namene testiranja programske opreme. Podatke za testiranje (testna in pred-produkcijska okolja) je treba anonimizirati, saj do njih lahko dostopajo

le pooblaščene osebe. Potrebo po revizijski sledi je predstavil že Informacijski pooblaščenec Republike Slovenije (2015) v smernicah za zavarovanje informacijskih podatkov, opredeljuje pa jo tudi GDPR.

4 ŠTUDIJA PRIMERA

4.1 Metodologija

S študijo primera sem izvedel kvalitativno raziskavo, kjer sem se poglobil v zatečeno stanje primerov pred zakonskimi spremembami in način izvedbe dela za zagotovitev skladnosti z zakonskimi spremembami, z namenom ocene uspešnosti opravljenega dela, pri čemer sem v nadaljevanju teoretične ugotovitve povezal s konkretnima primeroma in povzel ugotovitve. Namen študije primera je bil povezati smernice managementa sprememb z zagatami, s katerimi smo se v organizaciji srečevali pri vpeljavi informacijske podpore za zagotavljanje skladnosti z uredbo GDPR in IDD, predvsem zaradi skopo definiranih zahtev in zahteve po preložitvi roka za implementacijo zahtev po IDD. Iz opravljene študije sem v nadaljevanju poskušal predlagati smernice za pisanje zakonskih sprememb.

Primera izhajata iz praktičnih izkušenj pri vpeljavi informacijske podpore za zagotavljanje skladnosti z zakonodajnimi spremembami, ki sem jih pridobil kot poslovni analitik v zavarovalnici. Pri delu sem sodeloval pri usklajevanju funkcionalnih specifikacij za razvoj zahtevanih rešitev v sklepalnih aplikacijah in pri testiranju implementirane rešitve. V okviru projekta sem se udeleževal tudi srečanj delovne skupine za IDD.

Študija primera je podprta s pregledom interne dokumentacije in z intervjuji ključnih deležnikov, ki so sodelovali na pri vpeljavi zahtev GDPR in IDD. Intervjuje sem izvedel neformalno v decembru 2018, po zaključku obeh projektov. Z razgovori z vodjo IT, direktorjem prodaje, direktorjem poslovne analize in pooblaščeno osebo za varstvo podatkov (DPO) sem pridobil poglobljen vpogled v management informatike ter vodenje projektov, povezanih z zakonodajnimi spremembami v organizaciji.

Študija primera ima več omejitev, ki izhajajo iz narave raziskovalnega okolja in moje vloge v organizaciji. Kot poslovni analitik nisem imel dostopa do vseh internih podatkov, saj so bili nekateri zaradi varovanja poslovnih skrivnosti dostopni le ožjemu krogu zaposlenih. Posledično se analiza opira na delno omejen nabor informacij, kar lahko vpliva na celovitost prikaza posameznih procesov. Dodatna omejitev izhaja iz neformalnega značaja intervjujev, pri katerih so bili odgovori intervjuvancev deloma podprti s subjektivnimi interpretacijami in osebnimi izkušnjami. Ker sem bil kot član projektne ekipe neposredno vključen v vpeljavo obravnavanih rešitev, lahko tudi moja lastna interpretacija dogodkov in izzivov odraža določeno stopnjo

subjektivnosti. Te omejitve je treba upoštevati pri razumevanju rezultatov študije primera in pri presoji njihove prenosljivosti na druge organizacijske kontekste ali druge organizacije.

4.2 Vpliv Splošne uredbe EU o varstvu podatkov pri obdelavi osebnih podatkov na informacijski sistem izbrane organizacije

Zavarovalnice so zaradi svoje narave pod strogim nadzorom različnih nadzornih institucij, kot sta Informacijski pooblaščenec Republike Slovenije in AZN. Za informacijski sistem zavarovalnice je ključno, da je varen, zanesljiv in povsem skladen z zakonodajo, kar pomeni, da je bilo že izhodiščno stanje obstoječega sistema na visoki ravni varovanja osebnih podatkov. Za zavarovalnice je zahteve po varstvu osebnih podatkov narekoval že ZZavar-1, ki je še nadalje zaostril zahteve iz dosedanjega ZVOP-1.

4.3 Vpliv Splošne uredbe EU o varstvu podatkov pri obdelavi osebnih podatkov na procese v poslovanju

Z uvedbo GDPR ne spreminjamo temeljnih procesov zavarovalništva. Poslovne procese zavarovalništva lahko neovirano opravljamo ne glede na stanje privolitve o obdelavi osebnih podatkov – z osebnimi podatki razpolagamo po t. i. zakonitem interesu (Evropska komisija, brez datuma c).

Kot sem poudaril že v predhodnih poglavjih, so osebni podatki pomemben del prodajnega procesa in trženjskih kampanj. Stranko najlažje nagovorimo k oddaji privolitve za obdelavo osebnih podatkov ob sklepanju zavarovanj. Glavnino prodaje zavarovanj še vedno predstavljajo ustaljene prodajne poti, kot so lastna prodajna mreža in pogodbeni prodajniki. Manjši delež prodaje predstavlja spletno sklepanje. Letno poročilo Zavarovalnice Triglav, d. d., navaja, da je bilo v letu 2023 preko spleta sklenjenih 10 % vseh zavarovanj (Zavarovalnica Triglav, d. d., 2024).

Privolitev obdelave osebnih podatkov je bila po obstoječem sistemu »privzete privolitve«, kar pomeni, da se je stranka s podpisom zavarovalne pogodbe strinjala z obdelavo osebnih podatkov. Na pogodbi je bila namreč napisana klavzula o obdelavi osebnih podatkov, s katero se podpisnik ob podpisu strinja. Zajem privolitve o obdelavi osebnih podatkov je bil torej pasiven. Prodajnik, običajno je bil to zavarovalni zastopnik, z zajemom privolitve o obdelavi osebnih podatkov ni imel dodatnega dela, saj je bila privolitev del zavarovalne pogodbe. Če se stranka s klavzulo o obdelavi osebnih podatkov ni strinjala, je lahko pisno zahtevala preklic obdelave, kar je lahko storila že takoj po sklepanju pogodbe. GDPR ne dovoljuje več pridobivanja privolitev po načinu privzete privolitve, ampak mora biti privolitev za obdelavo pridobljena na aktiven način (Pirc Musar & partnerji, 2017), prav tako privolitev ne sme biti

pogojena z uporabo ponujene storitve, v našem primeru s sklenitvijo zavarovanja. Nadalje GDPR upravljavcem nalaga, da mora biti preklic obdelave osebnih podatkov enako enostaven, kot je bila privolitev za obdelavo.

V zavarovalnici je bila s strani prodaje zavarovanj sprejeta odločitev, da je treba posel nadaljevati neodvisno od zbiranja privolitev za obdelavo osebnih podatkov. V procesu sklepanja zavarovanja to pomeni, da se najprej sklene zavarovanje, preden pa se dokumenti podpišejo, se stranki ponudi tudi privolitev za obdelavo osebnih podatkov.

4.4 Vpeljava podpore za skladnost s Splošno uredbo EU o varstvu podatkov pri obdelavi osebnih podatkov

4.4.1 Vnos privolitev o obdelavi osebnih podatkov

V prejšnjem načinu dela so se privolitve strank beležile ročno v registru strank, kar je pomenilo, da je bilo treba stranke, ki so preklicale privolitev, ročno izključiti iz vseh sistemskih obdelav osebnih podatkov. Z uvedbo skladnosti z GDPR je bil vzpostavljen strukturiran pristop k upravljanju privolitev, ki vključuje tri ločene sklope, za katere lahko posameznik poda privolitev:

- Obdelavo osebnih podatkov (segmentirano (neposredno) trženje, vključno z oblikovanjem profila).
- Posredovanje osebnih podatkov »povezanim družbam« (posredovanje podatkov stranke družbam v skupini).
- Preverjanje popolnosti, točnosti in ažurnosti podanih osebnih podatkov.

Stranka lahko poda privolitev za vse sklope ali zgolj za posameznega. Ker imajo stranke pri zavarovalnici pogosto sklenjenih več zavarovanj, se v koledarskem letu večkrat srečajo z različnimi poslovnimi procesi zavarovalnice. Čeprav si organizacija prizadeva pridobiti čim večje število privolitev, bi pretirano ali ponavljajoče se pozivanje k podaji privolitve lahko negativno vplivalo na zaupanje strank, zato je bilo uvedeno pravilo, da sistem po zavrnitvi privolitve določen čas ne ponudi ponovne možnosti za njeno podajo.

Pridobivanje soglasij smo omogočili na več vstopnih točkah:

- Sklepanje zavarovanja preko prodajnega zastopnika.
- Sklepanje zavarovanja preko prodajnega komercialista.
- Sklepanje zavarovanja preko partnerske mreže (lizingi).
- Sklepanje zavarovanja preko spleta.

– Prijava škode preko škodnega centra.

Ker gre za lastno razvite programske rešitve, se je podpora za vnos privolitev razvijala interno. V praksi smo morali podporo zajema privolitev o obdelavi osebnih podatkov zagotoviti v zalednem sistemu in dveh sklepalnih aplikacijah. V zalednem sistemu, ki preko namenske aplikacije podpira vnos in urejanje strank, smo interno razvili ločen modul, ki skrbi za vnos in pregled stanja privolitev o obdelavi osebnih podatkov. V tem modulu se urejajo tudi morebitni preklici privolitve o obdelavi osebnih podatkov.

Zaradi časovne stiske so v prodaji zavarovanj sprejeli poslovno odločitev, da se v začetni fazi zagotovi podpora za aktivno zbiranje privolitev za zastopnike, saj ima zastopniška mreža največ stika s strankami in predstavlja glavnino prometa sklenjenih zavarovanj. Ključna za ves nadaljnji razvoj je bila zagotovitev podpore v zalednem sistemu, saj bi lahko v primeru, da nam ne bi uspelo pravočasno razviti rešitve za ostale sklepalne aplikacije, kljub vsemu vnašali pridobljene privolitve neposredno v zaledni sistem.

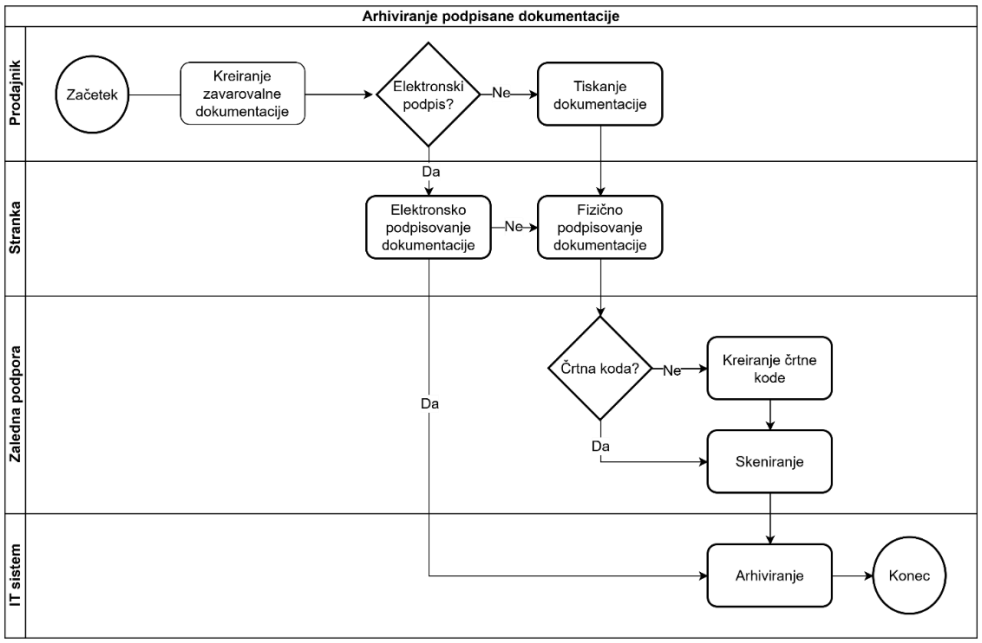
Strankam je bila omogočena tudi podaja privolitve neodvisno od sklepanja zavarovalnega posla. Ta možnost je podprta v zaledni aplikaciji, v aplikaciji za zastopnike in na spletnem portalu za stranke. Na spletni strani zavarovalnice je na voljo tudi obrazec, ki ga lahko stranka natisne in pošlje po pošti.

Ob uveljavitvi zakonskega roka za skladnost z GDPR so bila vsa obstoječa soglasja obravnavana kot neveljavna, saj so bila pridobljena na podlagi privzete privolitve. Izjema so bile zgolj novejše nagradne igre, pri katerih je bil že uporabljen mehanizem aktivne privolitve, skladen z zahtevami GDPR.

4.4.2 Vnos privolitve v ločenem modulu v zalednem sistemu baze strank

Za namen evidentiranja, pregleda in upravljanja sprememb privolitev za obdelavo osebnih podatkov je bil v aplikaciji za upravljanje baze strank razvit specializiran modul za vodenje privolitev. V modul se beležijo vse prejete privolitve, bodisi z ročnim vnosom bodisi s sistemskim prenosom, prav tako pa se vanj ročno vnašajo morebitni preklici privolitve. Vse privolitve in preklici, prejeti v fizični obliki, so vključeni v postopek digitalizacije ter shranjeni v dokumentni sistem, do katerega je mogoče dostopati prek povezave v modulu za vodenje privolitev. Dokumenti, podpisani z elektronskim podpisom, se shranijo neposredno v dokumentni sistem, brez potrebe po dodatni obdelavi.

Slika 2: Shema procesa digitalizacije dokumentov



Vir: lastno delo.

Postopek digitalizacije dokumentov, kot prikazuje slika 2, se uporablja za digitalizacijo ročno podpisanih zavarovalnih dokumentov. Fizične dokumente zaposleni ali pogodbeni partnerji pošljejo na centralno točko za digitalizacijo, kjer se dokumenti skenirajo in arhivirajo na ustrezno mesto v dokumentnem sistemu. Za pospešitev razporejanja skeniranih dokumentov je večina dokumentov opremljenih s črtno kodo, ki omogoča samodejno razvrščanje dokumentacije. Dokumente brez črtne kode je treba pred digitalizacijo ročno opremiti z ustrezno črtno kodo, da se zagotovi pravilna umestitev v dokumentni sistem.

4.4.3 Vnos privolitve v aplikaciji zalednega sistema za sklepanje zavarovanj

Aplikacija zalednega sistema omogoča izvajanje vseh operacij, potrebnih za sklepanje zavarovalnih pogodb in za izvedbo morebitnih kasnejših popravkov. Uporabniki te aplikacije so praviloma bolj izkušeni pri sklepanju zavarovanj kot uporabniki drugih sklepalnih aplikacij. Rešitev temelji na integraciji več zalednih sistemov, in sicer sistema za sklepanje zavarovanj ter sistema za upravljanje baze strank. V okviru rešitve je implementirano pravilo, ki pred tiskanjem zavarovalne dokumentacije preveri, ali je stranka podala popolno privolitev za obdelavo osebnih podatkov, pri čemer se upošteva tudi že opisano pravilo o časovnem zamiku ponovnega zbiranja privolitev v primeru predhodne zavrnitve.

V tem koraku je izbira odgovora obvezna. Če uporabnik izbere možnost »Želi«, aplikacija za sklepanje zavarovanj samodejno preusmeri uporabnika v modul za vnos privolitev v aplikaciji za upravljanje baze strank. Po uspešnem vnosu privolitve sistem samodejno preusmeri uporabnika nazaj v zaledno aplikacijo za sklepanje zavarovanj. Če uporabnik izbere možnost »Ne želi«, se ta odločitev zabeleži in se sproži pravilo o časovnem zamiku ponovnega pozivanja k podaji privolitve. Privolitev se stranki izroči skupaj s preostalo zavarovalno dokumentacijo.

Sklepalni aplikaciji za zastopnike in partnersko mrežo sta morali biti zasnovani bistveno enostavneje, saj ju uporabljajo uporabniki z različnimi stopnjami tehničnega znanja. Enako velja za spletno sklepanje zavarovanj, kjer je stranka praviloma prepuščena samostojni uporabi, zato mora biti uporabniška izkušnja posebej intuitivna in pregledna.

4.4.4 Vnos privolitve k obdelavi osebnih podatkov v aplikaciji za zavarovalne zastopnike

Zavarovalni zastopniki pri sklepanju zavarovalnih poslov uporabljajo ločeno sklepalno aplikacijo, ki je prilagojena njihovim delovnim procesom, enostavna za uporabo in opremljena z vgrajenimi mehanizmi, ki uporabnika vodijo skozi celoten postopek izvedbe posla. Rešitev temelji na podpori modula za vnos soglasij in preklicev v aplikaciji zalednega sistema, s katerim je integrirana.

V sklepalni aplikaciji se preverjanje statusa privolitve izvede z generiranjem računa. Tudi v tem primeru sistem uporabniku ponudi možnosti »Želi« in »Ne želi«. Ob potrditvi privolitve se izvede zapis v modul za upravljanje privolitev, dokument o privolitvi pa se stranki izroči skupaj s preostalo zavarovalno dokumentacijo.

Dodatno je bila v aplikaciji za zavarovalne zastopnike uvedena ločena funkcionalnost, ki omogoča vnos privolitve za obdelavo osebnih podatkov tudi izven postopka sklepanja zavarovalnega posla. Pri tem se uporablja ista storitev za vnos privolitve, vendar kot samostojen proces z ločenim uporabniškim vmesnikom. V takšnih primerih stranka prejme zgolj podpisan dokument o privolitvi za obdelavo osebnih podatkov, brez spremljajoče zavarovalne dokumentacije.

4.4.5 Vnos privolitve k obdelavi osebnih podatkov v aplikaciji za partnersko mrežo

Razvoj aplikacije za partnersko mrežo je potekal z zamikom glede na rok za skladnost z GDPR. Za ta prodajni kanal je bila namreč sprejeta poslovna odločitev, da se podpora za vnos privolitev za obdelavo osebnih podatkov lahko razvije v kasnejši fazi, ko bodo na voljo ustrezni viri v oddelku informatike. Privolitve za trženjske namene smo v tem obdobju lahko pridobivali tudi posredno – preko privolitev, ki so jih stranke podale našim poslovnim partnerjem.

Ob uveljavitvi GDPR digitalno podpisovanje v partnerski mreži še ni bilo podprto, zato je bila strankam poleg zavarovalne dokumentacije izročena tudi predtiskana fizična različica obrazca za privolitev k obdelavi osebnih podatkov. Vsa tiskana dokumentacija se je nato posredovala na centralno skenirno mesto, kjer je bila digitalizirana in arhivirana.

V kasnejši fazi je bila v aplikaciji za partnersko mrežo uvedena podpora za vnos privolitev. Sprva je bilo omogočeno izpolnjevanje obrazca za privolitev neposredno v aplikaciji, pri čemer se je na dokument samodejno dodala črtna koda, ki je omogočala učinkovito skeniranje in razporejanje dokumentacije. S povečanjem obsega prometa preko partnerske mreže pa se je pojavila potreba po uvedbi elektronskega podpisovanja dokumentov.

Odločitev za postopno digitalizacijo podpore GDPR v partnerskem kanalu odraža principe okvira Val IT, saj je bila najprej zagotovljena podpora v zastopniški prodajni poti, kjer je obseg prodaje največji, šele nato pa v drugih prodajnih kanalih. Na podlagi analize potrebnih virov za razvoj programske podpore je prodaja sprejela odločitev, da se razvoj funkcionalnosti za partnersko mrežo prestavi v drugo fazo, ko bodo sproščeni ustrezni IT-viri. V tej fazi je bila poleg podpore za zbiranje privolitev uvedena tudi možnost elektronskega podpisa dokumentov.

Uvedba elektronskega podpisovanja je omogočila zmanjšanje tveganja izgube dokumentacije, izboljšala natančnost podatkov ter znižala stroške, saj ni bilo več potrebno fizično pošiljanje dokumentacije in njeno skeniranje na centralni lokaciji. Kljub temu ročno podpisovanje ni bilo ukinjeno in ostaja rezervna možnost za stranke, ki elektronskega podpisa ne želijo uporabljati. Fizični podpis je še posebej pogost pri starejših strankah, ki se pogosto počutijo bolj varno pri tradicionalnih načinih potrjevanja dokumentov.

4.4.6 Beleženje pogledov v osebne podatke strank

Kot temelj za vzpostavitev sistema beleženja vpogledov v osebne podatke strank je služila že obstoječa funkcionalnost v zalednih sistemih. Ta je bila za potrebe zagotavljanja skladnosti z GDPR nadgrajena z dodatno podporo beleženja prikaza osebnih podatkov v sklepalnih aplikacijah.

Za zagotovitev revizijske sledi in zaznavanje morebitnih nepooblaščenih vpogledov v osebne podatke smo uvedli sistem beleženja vseh vpogledov zaposlenih v podatke strank. Pri načrtovanju tega sistema smo se soočili z izzivom obvladovanja velike količine podatkov, ki bi lahko predstavljala znatno obremenitev shranjevalnih kapacitet. Zato je bila implementirana rešitev, ki namesto beleženja vseh prikazanih rezultatov iskanja evidentira zgolj izvedene poizvedbe v iskalniku.

Sistem za beleženje vpogledov tako poleg vpogleda v posamezno stranko beleži tudi podatke o iskalnih rezultatih, na podlagi katerih je bila stranka prikazana. Pri iskanju določene osebe se namreč med rezultati iskanja prikažejo osnovni osebni podatki vseh posameznikov z enakim imenom in priimkom. Obseg prikazanih podatkov se razlikuje glede na namembnost posamezne aplikacije: v aplikacijah partnerske mreže je praviloma viden zgolj naslov stranke, medtem ko zaledni sistemi omogočajo prikaz širšega nabora osebnih podatkov, ki omogočajo natančnejšo identifikacijo oziroma razlikovanje med posamezniki.

4.4.7 Anonimizacija podatkov

Pri razvoju programske opreme je ena ključnih faz testiranje zgrajene rešitve. Black (2014) ugotavlja, da so testna okolja praviloma manjša od produkcijskih, pri uporabi produkcijskih podatkov pa organizacije pogosto omejuje zakonodaja. Luo (2001) poudarja, da je za zanesljivo oceno kakovosti programske opreme v realnih ali simuliranih okoliščinah bistvena uporaba podatkov, ki so čim bolj podobni dejanskim.

Za zagotovitev takšne realističnosti se v testne namene izvaja anonimizacija produkcijskih podatkov (Murthy in drugi, 2019). Pri tem se anonimizira baza strank, tako da posamezniki po obdelavi niso več določljivi. Testiranje se tako lahko izvaja na realnih primerih, ki vključujejo raznolike scenarije, ki bi jih bilo sicer težko predvideti. Osebni podatki niso potrebni zgolj pri testiranju programske opreme, temveč tudi pri razvoju novih zavarovalnih produktov. Anonimizacija se izvaja tudi pri zgodovinskih podatkih, kjer zakonodaja po preteku roka hrambe zahteva izbris ali nepovratno anonimizacijo osebnih podatkov. Pri zgodovinskih podatkih je ključna informacija povezana z dogodkom, ne pa z identiteto posameznika, zato je anonimizacija smiselnejša od izbrisa.

Psevdonimizacija osebnih podatkov je bila uvedena v vseh podatkovnih bazah, ki niso del produkcijskega okolja. Za razvoj in testiranje programske opreme osebni podatki posameznih strank niso potrebni. Z uvedbo psevdonimizacije se zmanjšuje tveganje, ki ga predstavlja obdelava osebnih podatkov v neprodukcijskih okoljih (Van Deursen in Kummeling, 2019). Psevdonimizacija se izvaja periodično, in sicer s postopkom mešanja podatkov ob prepisovanju baze, pri čemer se podatki premešajo znotraj posameznih stolpcev.

4.4.8 Vodenje zbirk podatkov

Za zagotovitev skladnosti z GDPR je bil nadgrajen tudi sistem za vodenje zbirk podatkov. Razvoja aplikacije za to funkcionalnost se organizacija ni lotila interno, temveč je rešitev poiskala na trgu in izbrala zunanjega ponudnika, specializiranega za tovrstne sisteme. Takšna odločitev odraža raznolikost in kompleksnost informacijskega okolja v organizaciji, ki temelji

na kombinaciji lastno razvitih rešitev in komercialne programske opreme. Integracija obeh pristopov omogoča učinkovitejše upravljanje informacijskih procesov, hkrati pa zagotavlja skladnost z regulativnimi zahtevami.

4.4.9 Dodatna dela za zagotovitev skladnosti s Splošno uredbo EU o varstvo podatkov pri obdelavi osebnih podatkov

S prihodom zakonskega roka za zagotovitev skladnosti z GDPR se aktivnosti na področju skladnosti niso zaključile. Zagotavljanje skladnosti je postalo redna in trajna naloga, ki vključuje stalno spremljanje pravilnega delovanja vzpostavljenih sistemov in kontrol. Zahtev GDPR ni dopustno zanemariti niti pri razvoju novih funkcionalnosti programske opreme niti pri vzpostavljanju sodelovanja z novimi poslovnimi partnerji.

Med dodatnimi aktivnostmi, izvedenimi po 25. 5. 2018, velja izpostaviti dva primera: prenovo dokumenta za podajo privolitve za obdelavo osebnih podatkov in uvedbo soglasja za oddaljeno podpisovanje, pri katerem je stranka v fazi podpisovanja preusmerjena k zunanjemu izvajalcu.

Prenova dokumenta za oddajo privolitve priča o tem, da zahteve niso bile v celoti razumljene, zato je bila izbrana rešitev, ki je bila v tistem času ocenjena kot najvarnejša. Poleg prenove samega dokumenta je bilo treba zagotoviti tudi ustrezno podporo v vseh sklepalnih aplikacijah in zalednih sistemih. Iz dokumenta o privolitvi je bila odstranjena točka, ki se je nanašala na preverjanje popolnosti, točnosti in ažurnosti osebnih podatkov. Dodatno je bila prepoznana zahteva, da mora biti uporabnik v primeru oddaljenega podpisovanja, ki poteka preko zunanjega ponudnika, izrecno seznanjen s tem, da bodo njegovi osebni podatki posredovani pogodbenemu obdelovalcu. Če stranka s tem ne soglaša, postopka oddaljenega podpisovanja ni mogoče izvesti.

Zaradi vključitve zunanjega ponudnika za oddaljeno podpisovanje je bilo treba stranki pred izvedbo podpisnega postopka ponuditi posebno izjavo, s katero potrdi strinjanje s posredovanjem podatkov in uporabo storitve zunanjega izvajalca. V primeru zavrnitve tak način podpisovanja ni mogoč. Ta funkcionalnost je bila implementirana tako v aplikaciji za zavarovalne zastopnike kot v aplikaciji za partnersko mrežo.

4.5 Vpeljava podpore za skladnost z direktivo o distribuciji zavarovanj

IDD se nanaša na celoten proces sklepanja zavarovalnih pogodb, zato je bilo treba informacijsko podporo njenim zahtevam zagotoviti hkrati v vseh sklepalnih aplikacijah. Za doseganje skladnosti z direktivo je bilo nujno implementirati podporo za izpolnjevanje testa potreb in zahtev (t. i. IDD vprašalnika) ter zagotoviti, da sta tako IDD vprašalnik kot dokument IPID vključena med izhodne dokumente v vseh prodajnih kanalih.

Pri oblikovanju IDD vprašalnika je bilo v okviru delovne skupine zavarovalnega združenja dalj časa odprto vprašanje, ali naj test potreb in zahtev ugotavlja tako potrebe kot zahteve stranke ali pa bo zadostovalo zgolj evidentiranje potreb, ki bi se posredno interpretirale tudi kot zahteve. Ker do enotnega dogovora ni prišlo pravočasno, da bi lahko rešitev ustrezno informacijsko podprli, je projektna skupina sprejela odločitev, da se test potreb in zahtev implementira v celoti, skladno z izhodišči direktive.

V okviru prizadevanj za poenotenje dokumenta z informacijami o zavarovalnem produktu je EIOPA februarja 2017 predstavila osnutek dokumenta IPID, ki je služil kot temelj za oblikovanje vseh nadaljnjih različic. V delovni skupini zavarovalnega združenja je bil sprejet dogovor, da lahko zavarovalnice v Republiki Sloveniji na dokumentu IPID uporabljajo svoje zaščitne barve. Takšna rešitev naj bi zavarovancem olajšala primerjavo produktov med posameznimi zavarovalnicami ter prispevala k večji preglednosti in razumljivosti informacij (EIOPA, 2017).

4.5.1 Proces sklepanja zavarovanj pred direktivo o distribuciji zavarovanj in tveganja za stranko

Proces sklepanja zavarovanj pred uvedbo IDD je bil razmeroma preprost in je v veliki meri temeljil na zaupanju med prodajnikom in stranko. Takšen odnos je prodajnika pogosto postavljal v nadrejeni položaj, kar je lahko vodilo do asimetrije informacij in posledično do prodaje zavarovalnih produktov, ki jih stranka ni dejansko potrebovala. IDD je bila uvedena prav z namenom zmanjšanja teh tveganj ter vzpostavitve bolj uravnoteženega, preglednega in potrošniku prijaznega prodajnega procesa.

4.5.2 Izdaja dokumenta z informacijami o zavarovalnem produktu

Pri izdaji IPID-a se je zavarovalnica soočila z dilemo glede ustreznega trenutka njegove izročitve stranki. Tradicionalni prodajni proces je namreč predvideval, da se vsa dokumentacija podpiše in izroči šele ob zaključku sklepanja zavarovalnega posla, kar pa po zahtevah IDD ni več sprejemljivo. Direktiva namreč zahteva, da je stranka z bistvenimi informacijami o produktu seznanjena že pred sprejemom odločitve o sklenitvi zavarovanja.

Zato je bil prodajni proces ustrezno prilagojen. Prodajnik mora stranki že ob predstavitvi posameznega zavarovalnega produkta omogočiti vpogled v pripadajoči dokument IPID. V trajno last pa stranka prejme IPID skupaj s preostalo zavarovalno dokumentacijo ob sklenitvi zavarovalne pogodbe. V primerih, ko do sklenitve zavarovalnega posla ne pride, ima zastopnik možnost, da stranki IPID natisne preko namenske aplikacije, s čimer se zagotovi izpolnjevanje obveznosti informiranja tudi v takšnih situacijah.

4.5.3 Test potreb in zahtev in razhajanje s polico

Direktiva zahteva, da je zavarovanje sklenjeno na podlagi dejanskih potreb in zahtev stranke. Zato je bilo v sklepalnih aplikacijah treba zagotoviti celovito podporo procesu izpolnjevanja testa potreb in zahtev (IDD vprašalnika). V praksi se pogosto zgodi, da se stranka med postopkom sklepanja zavarovanja odpove posameznim kritjem zaradi nižje cene, kar pomeni, da lahko obstaja potreba, ki pa ne predstavlja tudi strankine zahteve. Če stranka določeno kritje v vprašalniku označi kot zahtevo, kasneje pa tega kritja ne izbere, nastane razhajanje med izpolnjenim vprašalnikom in sklenjenim zavarovanjem.

Za obravnavo takšnih primerov je bila v zaledni del sklepalne aplikacije implementirana logika, ki preverja skladnost sklenjene police z izpolnjenim IDD vprašalnikom. Ob ugotovljenem razhajanju sistem prodajnika opozori in zahteva vnos komentarja z utemeljitvijo odstopanja. Razlog za razhajanje se skupaj s številko IDD vprašalnika zapiše na zavarovalno polico, kar zagotavlja sledljivost in transparentnost postopka.

Za vzpostavitev programske podpore IDD vprašalnika je bilo v zalednem sistemu najprej treba vzpostaviti povezave med posameznimi vprašanji in ustreznimi zavarovalnimi kritji. Na podlagi teh povezav je bilo mogoče preverjati skladnost med izraženimi potrebami in zahtevami stranke ter dejansko sklenjenim zavarovanjem.

Test potreb in zahtev je bil implementiran tako, da se potrebe in zahteve izpolnjujejo ločeno – v dveh stolpcih, izpolnjenega vprašalnika pa v sklepalnih aplikacijah ni več mogoče spreminjati. Izjema je le popolna prekinitev postopka sklepanja in ponovni začetek, kar zagotavlja verodostojnost podanih odgovorov. Stranka lahko izpolnjevanje IDD vprašalnika tudi zavrne; v tem primeru se generira izjava o zavrnitvi. V obeh primerih mora stranka podpisati dokument, ki se nanaša na IDD vprašalnik – bodisi opravljen test potreb in zahtev bodisi izjavo o zavrnitvi. Referenčna številka IDD vprašalnika (ali izjave o zavrnitvi) se zapiše tudi na zavarovalno polico.

Pri podpisovanju dokumentacije je bil sistemsko zagotovljen ustrezen vrstni red, tako da se IDD vprašalnik vedno podpiše pred zavarovalno polico. Na ta način se zagotovi skladnost s procesnimi in regulativnimi zahtevami.

5.5.4 Kreiranje police na podlagi izpolnjenega vprašalnika

Glede na stroge zahteve IDD je bilo smiselno razmisliti o poenostavitvi procesa sklepanja zavarovanj z aktivnim vključevanjem testa potreb in zahtev v sam prodajni postopek. Tak pristop bi omogočal sočasno izpolnjevanje vprašalnika in oblikovanje zavarovalne police, s

čimer bi se odpravila razhajanja med izraženimi zahtevami stranke in dejansko sklenjenim zavarovanjem. Sistem bi tako lahko vedno ponudil produkt, ki bi najbolj ustrezal potrebam in zahtevam posamezne stranke.

Analiza časovnice in razpoložljivih virov je pokazala, da so obstoječi zavarovalni produkti preveč kompleksni, da bi bilo mogoče zavarovalno polico avtomatsko generirati neposredno iz IDD vprašalnika. Zato je bila sprejeta odločitev, da se takšen pristop uvede postopoma, in sicer ob predstavitvi novih ali prenovi obstoječih zavarovalnih produktov. Prva realizacija tega koncepta je bila izvedena leta 2021 s prenovljenim produktom za zavarovanje nepremičnin.

Z uvedbo nove sklepalne aplikacije je bilo leta 2025 omogočeno tudi sklepanje avtomobilskega zavarovanja na podlagi izpolnjenega IDD vprašalnika, pri čemer sistem samodejno predlaga ustrezna zavarovalna kritja. Predvidoma bo v letu 2026 enak način sklepanja podprt tudi za druge ključne zavarovalne produkte, ki bodo vključeni v novo generacijo sklepalnih aplikacij.

4.5.5 Ostali zahtevani ukrepi za skladnost z direktivo o distribuciji zavarovanj

IDD med drugim zahteva tudi redno izobraževanje zavarovalnih zastopnikov. Ti morajo poleg dovoljenja za opravljanje poslov zavarovalnega zastopanja vsako leto opraviti najmanj 15 ur dodatnega usposabljanja s širšega področja zavarovalništva, kar morajo dokazati z ustreznimi potrdili (Slovensko zavarovalno združenje, 2018). Za podporo izpolnjevanju teh zahtev je bil sistem za izobraževanje in upravljanje s kadri dopolnjen z evidenco in vsebinsko podporo za t. i. IDD izobraževanja.

Z lastnim razvojem je bila v zavarovalnici vzpostavljena tudi aplikacija, ki omogoča enostaven in centraliziran dostop do zavarovalnih pogojev ter cenikov. V okviru te aplikacije je bila podprta tudi uvedba novega dokumenta, ki ga zahteva direktiva – IPID. Aplikacija zavarovalnim zastopnikom omogoča, da imajo vedno dostop do najnovejših pogojev, cenikov in dokumentov IPID, kar bistveno izboljšuje kakovost in konsistentnost informacij, posredovanih strankam.

Z uvedbo namenske aplikacije sta bila zastopnikom omogočena hitro iskanje in dostop do relevantnih informacij, hkrati pa je bila odpravljena potreba po hranjenju kopij dokumentov na lokalnih računalnikih. S tem je organizacija pridobila nadzor nad uporabo dokumentacije ter zagotovila, da so v obtoku vedno ažurne in pravilne različice dokumentov. Aplikacija omogoča tudi enostavno tiskanje ali elektronsko posredovanje dokumenta IPID še pred začetkom postopka sklepanja zavarovanja, kar dodatno krepi skladnost z zahtevami IDD.

4.6 Povzetek izvedenih sprememb

Za zagotovitev skladnosti z GDPR je bil nadgrajen sistem za beleženje revizijske sledi vpogledov v osebne podatke. Nadgradnja je obsegala beleženje rezultatov iskanja, uvedbo psevdonimizacije v vseh neprodukcijskih okoljih in vzpostavitev sistema za vodenje zbirk osebnih podatkov. Poleg tega je bila implementirana celovita podpora za vnos in spremljanje GDPR-soglasij v vseh sklepalnih, podpornih in zalednih aplikacijah. Zaradi uvedbe novega sistema zbiranja soglasij so bila vsa predhodno pridobljena soglasja preklicana. Med ključnimi nalogami je bilo tudi oblikovanje vsebine soglasij za obdelavo osebnih podatkov, priprava IPID-ov za vse zavarovalne produkte ter oblikovanje ustreznih vprašanj za test potreb in zahtev po posameznih zavarovalnih vrstah.

Skladnost z GDPR je bila v zavarovalnici izvedena projektno. Projekt je trajal šest mesecev, pri čemer je bilo za razvoj in podporo porabljenih več kot 4000 projektnih ur. Približno 20 % vseh stroškov je predstavljal nakup programske opreme za vodenje evidenc osebnih podatkov.

Ker je bil rok za skladnost z IDD prestavljen, se je bilo mogoče do roka za uvedbo GDPR v celoti posvetiti zahtevam uredbe, z implementacijo IDD pa nadaljevati po tem datumu. Za zagotovitev skladnosti z IDD je bila vzpostavljena aplikacijska podpora za izpolnjevanje testov potreb in zahtev ter za upravljanje IPID-ov.

Za izpolnjevanje zahtev IDD je bilo v zavarovalnici treba definirati nova poslovna pravila za sklepanje zavarovanj. Eno izmed ključnih odprtih vprašanj, obravnavanih na delovnem telesu, je bilo, ali naj obrazec za test potreb in zahtev ločeno naslavlja potrebe in zahteve ali naj se potrebe posredno interpretirajo kot zahteve. Ker je dokument postal obvezni del zavarovalne dokumentacije, je bilo treba izpolnjevanje in izpis vprašalnika programsko podpreti v vseh sklepalnih aplikacijah. Enak prodajni postopek, kot ga zahteva direktiva, se izvaja tudi pri informativnih ponudbah.

Na podlagi odgovorov stranke v testu potreb in zahtev bi bilo mogoče zavarovalni produkt ponuditi sistemsko, neposredno iz zavarovalne aplikacije, kar bi zagotovilo skladnost sklenjene police z izraženimi zahtevami stranke ter razbremenilo zavarovalnega zastopnika. Trenutni proces zahteva najprej izpolnitev vprašalnika, ki ga stranka lahko tudi zavrne, šele nato sledi sklepanje police. Zato je bila sprejeta odločitev, da se ta koncept postopno uvede pri novih ali prenovljenih produktih, kar se je že začelo uresničevati v letih 2021, 2025 in 2026.

Pri implementaciji zahtev GDPR je zavarovalnica zavestno izbrala pristop, ki upošteva najstrožje zakonske zahteve. Takšna strategija je omogočila izogibanje kasnejšim obsežnim nadgradnjam informacijskega sistema, ki bi zahtevale dodatne razvojne vire in upočasnile

izvajanje tekočih poslovnih pobud. Podpora za pridobivanje soglasij je bila zasnovana na načelu največje dodane vrednosti: najprej je bila uvedena v zastopniški mreži, kjer poteka največji del poslovnih aktivnosti in kjer je mogoče uporabnike tudi najučinkoviteje motivirati k podaji soglasij. Preostali prodajni kanali so bili vključeni postopoma, ko je časovni pritisk popustil in so bili ponovno na voljo ustrezni razvojni viri.

4.7 Ključne ugotovitve študije primera

Pri vpeljevanju informacijske podpore za zagotavljanje skladnosti z obema zakonskima spremembama smo morali hkrati vzpostaviti tudi procese, ki so bili prepoznani kot ključni za izpolnjevanje zahtev evropskih regulativ. V prodajni proces je bilo treba vključiti izpolnjevanje testa potreb in zahtev, zbiranje privolitev za obdelavo osebnih podatkov ter prilagoditi proces podpisovanja dokumentacije. Navedene spremembe je mogoče umestiti v ITIL-dimenzijo »vrednostnih tokov in procesov«, saj so zahtevale celovito prenovo obstoječih delovnih tokov ter njihovo integracijo v informacijski sistem. Prenovljeni prodajni proces je moral biti dodatno podprt z ustreznimi informacijskimi rešitvami, kar ustreza ITIL-dimenziji »informacije in tehnologija«. Pri tem je bilo ključno zagotoviti razpoložljivost in zanesljivost delovanja storitev, ustrezne ravni dostopnih pravic, varovanje informacij ter pravočasno posredovanje podatkov, kar izpostavlja tudi Agutter (2020).

Izzivi upravljanja informatike in sledenja zakonodaji so v literaturi že prepoznani, zato je uporaba ogrodij, kot sta ITIL in COBIT, še posebej smiselna (Karczewska, 2017). Poleg popolnoma novih zahtev pa so bile v GDPR vključene tudi nekatere zahteve, ki so sovpadale z obstoječimi standardi, kot sta ISO 27001 (GRO Solutions, 2025) in ISO 29100. To je organizacijam olajšalo izpolnjevanje varnostnih zahtev, saj so lahko izkoristile že vzpostavljene kontrole in procese ter tako zmanjšale obseg potrebnih prilagoditev. Podobno lahko z ITIL-dimenzijo »partnerji in dobavitelji« povežemo aktivnosti, ki so vključevale preverjanje skladnosti vseh zunanjih partnerjev, ki sodelujejo pri obdelavi osebnih podatkov. Prepričati smo se morali, da tudi partnerji delujejo v skladu z zahtevami GDPR, hkrati pa jim zagotoviti ustrezno podporo. Enako je veljalo pri implementaciji IDD, kjer smo sodelovali z zunanjimi prodajnimi partnerji in jim nudili podporo pri zagotavljanju skladnosti z direktivo. Primer takšnega sodelovanja je partner, ki za našo in druge organizacije izvaja storitve elektronskega in oddaljenega podpisovanja.

Hofstede in drugi (2011) izpostavljajo, da organizacijska kultura predstavlja ključen dejavnik pri vsakodnevnem delovanju organizacije, oblikovanju percepcij novih zaposlenih ter pri njeni zmožnosti odzivanja na spremembe v zunanjem okolju. V obravnavani organizaciji se je kot bistveno izkazalo, da zaposleni na vseh ravneh razumejo in sprejemajo pomen regulativnih

okvirov, kot sta GDPR in IDD, kar je mogoče neposredno povezati z ITIL-dimenzijo »organizacije in ljudje«.

Na vse štiri ITIL-dimenzije je izrazito vplival enoten zunanji dejavnik – pravni okvir. Tako GDPR kot IDD sta zahtevala obsežne prilagoditve informacijskih sistemov in procesov, pri čemer lahko vsak od teh regulativnih dejavnikov poseže v katerokoli dimenzijo upravljanja storitev ter s tem preoblikuje način, kako organizacija načrtuje, izvaja in izboljšuje svoje storitve.

Analiza primerov implementacije zakonodaje v Sloveniji – ZVOP-2, ZZavar-1A in ZZavar-1B – kaže, da ni bilo enotne časovnice za prenos evropskih zahtev v nacionalni pravni red. Medtem ko je od začetka veljavnosti GDPR do spremembe slovenskega zakona minilo več kot tri leta, je bila IDD v slovensko zakonodajo prenesena v nekaj mesecih. Primer ZZavar-1A in njegove dopolnitve ZZavar-1B dodatno razkriva, da se lahko zakonodajne zahteve v razmeroma kratkem obdobju – v tem primeru 17 mesecev – ponovno spremenijo. Bowman in Gufflet (2017) poudarjata, da je Evropska komisija osnutek uredbe predstavila že januarja 2012, nato pa je sledilo štiri leta in pol intenzivnih pogajanj, preden sta Svet EU in Evropski parlament potrdila končno besedilo, s čimer se je 27. aprila 2016 začelo dvoletno prehodno obdobje. Kljub obsežnosti zahtev in številnim vpletenim deležnikom uredba zahteva premišljen pristop ter zavezanost vodstva organizacij, hkrati pa predstavlja priložnost za celovit pregled obdelave podatkov in varnostnih politik znotraj organizacij.

Literatura dosledno poudarja ključno vlogo regulatorjev pri omogočanju učinkovite in avtomatizirane digitalne skladnosti. Butler in O'Brien (2019, str. 87) regulatorjem GDPR očitata pomanjkanje proaktivnosti v primerjavi s finančnimi regulatorji, kar je organizacije potisnilo v »pasti razdrobljenega pristopa babilonskega stolpa.« Podobno Ryan in drugi (2021) ugotavljajo, da bi morali nadzorni organi delovati kot osrednji omogočevalci in spodbujevalci razvoja RegTecha, vendar so to v kontekstu GDPR prevzeli razmeroma počasi, kar je povzročilo raznolike interpretacije in nejasna pričakovanja. Mohamed in Yildirim (2021) poudarjata, da je uvedba GDPR sprožila globalne regulativne premike, saj je spodbudila oblikovanje novih ter posodobljenih okvirov za varstvo osebnih podatkov z namenom ohranjanja nemotenega pretoka podatkov med različnimi pravnimi sistemi, kar potrjuje potrebo po tem, da zakonodajalci pri oblikovanju zahtev upoštevajo vpliv zakonodajnih sprememb na informacijske sisteme organizacij. Brez jasno definiranih in pravočasno podanih zahtev je namreč implementacija skladnosti v teh sistemih izjemno zahtevna. Iz primera vpeljevanja IDD pa je mogoče razbrati tudi pomen zgodnjega vključevanja in sodelovanja vseh deležnikov, skladno z načeli okvira GRC, kar omogoča bolj usklajeno, učinkovito in trajnostno izvajanje zakonodajnih sprememb.

Skupne ugotovitve potrjujejo, da zakonodajne spremembe, kot sta GDPR in IDD, pomembno in večplastno vplivajo na organizacije, saj posegajo v vse dimenzije upravljanja storitev – od procesov in tehnologije do partnerjev ter organizacijske kulture. Učinkovita implementacija skladnosti zahteva celovit pristop, ki presega zgolj tehnične prilagoditve informacijskih sistemov in vključuje prenovo delovnih tokov, okrepljeno sodelovanje z zunanjimi partnerji ter visoko stopnjo ozaveščenosti zaposlenih. Uporaba uveljavljenih ogrodij, kot sta ITIL in COBIT, ter sklicevanje na standarde, kot sta ISO 27001 in ISO 29100, pomembno olajšata obvladovanje zahtev in zmanjšata kompleksnost sprememb.

Iz študije primera je razvidno, da je uspešnost implementacije močno odvisna od pravočasnega, jasnega in usklajenega delovanja regulatorjev. Pomanjkanje proaktivnosti in nedosledna komunikacija lahko povzročita razdrobljene interpretacije ter otežita vključevanje zahtev v informacijske sisteme. Primeri iz prakse potrjujejo, da so organizacije uspešnejše, kadar zakonodajne zahteve zgodaj razumejo, jih sistematično vključijo v svoje procese ter zagotovijo aktivno sodelovanje vseh deležnikov, skladno z načeli okvira GRC. Celostni pristop k upravljanju skladnosti se tako izkaže kot ključen za učinkovito, trajnostno in organizacijsko zrelo odzivanje na regulativne spremembe.

Ključne ugotovitve magistrskega dela, strnjene v naslednje točke:

- Implementacija GDPR in IDD zahteva posege v vse štiri ITIL-dimenzije, kar potrjuje večplastnost vpliva zakonodaje na organizacije.
- Uporaba ogrodij ITIL, COBIT in GRC ter standardov ISO 27001 in ISO 29100 pomembno olajša obvladovanje kompleksnosti zakonodajnih sprememb.
- Organizacijska kultura in ozaveščenost zaposlenih sta ključna dejavnika uspešne implementacije skladnosti.
- Zunanje časovnice zakonodajnih sprememb so nepredvidljive, kar otežuje načrtovanje in zahteva visoko stopnjo prilagodljivosti informacijskih sistemov.
- Regulatorji imajo ključno vlogo pri zagotavljanju jasnih, pravočasnih in usklajenih interpretacij, ki so nujne za učinkovito digitalno skladnost.
- Sodelovanje z zunanjimi partnerji in dobavitelji je bistveno, saj morajo tudi oni izpolnjevati zahteve GDPR in IDD.
- Zgodnje vključevanje deležnikov in sistematično upravljanje sprememb zmanjšujeta tveganje naknadnih prilagoditev informacijskih rešitev.
- Zakonodajne spremembe predstavljajo tudi priložnost za izboljšanje procesov, varnostnih politik in upravljanja podatkov.

5 SKLEP

Pri vpeljavi informacijske podpore za izpolnjevanje zakonskih zahtev na ravni EU smo se v organizaciji soočili s številnimi izzivi. Proces je zahteval oblikovanje in uvedbo novega delovnega toka, razvoj dodatne aplikativne podpore pri sklepanju zavarovanj ter posodobitev sistema za upravljanje osebnih podatkov. Ti posegi so pomembno vplivali na časovni okvir razvojnih aktivnosti na področju informatike v organizaciji. Čeprav so bile temeljne zahteve opredeljene, se je med implementacijo tako novega delovnega procesa kot informacijske rešitve izkazalo, da obstaja veliko nepredvidenih vprašanj glede podrobnih specifikacij, ki jih v začetnih fazah ni bilo mogoče predvideti in so se razkrile šele med načrtovanjem. Odgovorni deležniki so ta vprašanja naslavljali na pristojne organe. Nekatere zahteve so bile v uredbah oziroma direktivah opredeljene relativno široko, kar je dopuščalo več možnih interpretacij, o določenih vidikih pa je razprava s predlagateljem zakonodaje še potekala. Ker bi lahko neodgovorjena vprašanja vodila do sprememb konceptualnih rešitev in s tem do potrebe po ponovnem začetku razvoja informacijske podpore, smo si prizadevali pridobiti čim več uradnih pojasnil pristojnih institucij.

Iz analize primerov ZVOP-2, ZZavar-1A in ZZavar-1B je razvidno, da v Sloveniji ni bilo enotne časovnice sprejemanja zakonodaje, kar je dodatno oteževalo pravočasno načrtovanje sprememb v organizacijah. V primeru GDPR je od datuma veljave evropske uredbe do spremembe zakona minilo več kot tri leta, medtem ko je bila IDD v slovensko zakonodajo umeščena v nekaj mesecih od začetka veljave evropske direktive. Razlike v časovnicah – od večletnih zamikov pri prenosu uredb do hitrih sprememb direktiv – ustvarjajo okolje, v katerem morajo organizacije delovati proaktivno in pogosto načrtovati na podlagi najstrožjih možnih interpretacij. Hkrati primer IDD razkriva, da se lahko zakonodajne zahteve v kratkem času tudi spremenijo, kar še povečuje potrebo po prilagodljivosti informacijskih sistemov in procesov.

Študija potrjuje tudi pomembno vlogo regulatorjev pri omogočanju učinkovite digitalne skladnosti. Literatura opozarja, da je bila pri GDPR vloga nadzornih organov pri podpori avtomatizirane skladnosti manj proaktivna, kar je organizacije postavilo pred izzive razdrobljenih interpretacij in nejasnih pričakovanj. To poudarja potrebo po bolj usklajenem, pravočasnem in nedvoumnem komuniciranju regulatorjev, zlasti v obdobjih intenzivnih zakonodajnih sprememb. Vpeljava zahtev je pokazala, da je sodelovanje deležnikov – poslovnih analitikov, pravnikov, službe skladnosti, prodaje in IT – ključno za uspešno implementacijo zahtev. Uporaba ogrodij, kot so ITIL, COBIT in GRC, ter sklicevanje na mednarodne standarde (npr. ISO 27001 in ISO 29100) sta se izkazala kot pomembna podpora pri obvladovanju kompleksnosti in zagotavljanju skladnosti, kar je razvidno predvsem iz primera zagotavljanja skladnosti z GDPR. Standardizirani pristopi omogočajo boljšo sledljivost, ponovljivost in preglednost procesov, kar je pri zakonodajnih spremembah bistvenega pomena.

Pri interpretaciji ugotovitev je treba upoštevati tudi omejitve študije primera. Zaradi varovanja poslovnih informacij kot poslovni analitik nisem imel dostopa do vseh internih virov, kar je vplivalo na obseg razpoložljivih podatkov in globino analize posameznih procesov. Del ugotovitev temelji na neformalnih intervjujih, pri katerih so bili odgovori intervjuvancev deloma oblikovani skozi prizmo njihovih osebnih izkušenj in subjektivnih interpretacij. Tudi moja lastna vloga v projektni ekipi lahko vpliva na razumevanje določenih odločitev in izzivov. Kljub tem omejitvam študija ponuja relevanten vpogled v kompleksnost zakonodajnih sprememb in njihovo implementacijo v informacijskih sistemih ter predstavlja izhodišče za nadaljnje raziskave na tem področju.

Ena izmed osrednjih ugotovitev magistrskega dela je, da bi lahko zakonodajalci pomembno zmanjšali časovni pritisk na organizacije, če bi zagotovili pravočasno, konsistentno in nedvoumno tolmačenje zahtev ter dali jasen signal, da bodo evropske zahteve prenesene brez dodatnih nacionalnih odstopanj. Zgodnejše vključevanje strokovnih delovnih teles bi omogočilo boljšo pripravo na spremembe in zmanjšalo tveganje za naknadne popravke informacijskih rešitev. Vodstvo organizacij bi moralo ob tem zagotoviti ustrezne vire in učinkovito upravljanje sprememb, saj je to ključno za uspešno in pravočasno implementacijo.

Skupni imenovalec analiziranih primerov je, da zakonodajne spremembe niso zgolj obveznost, temveč tudi priložnost za pregled in izboljšanje procesov, upravljanja podatkov ter varnostnih politik. Učinkovito upravljanje sprememb, podprto z jasnimi zahtevami in pravočasnim sodelovanjem deležnikov, omogoča organizacijam, da zakonodajne zahteve ne le izpolnijo, temveč jih izkoristijo kot vzvod za dvig kakovosti in zrelosti svojih informacijskih sistemov.

SEZNAM KLJUČNE LITERATURE

1. Agutter, C. (2020). *ITIL 4 essentials: your essential guide for the ITIL 4 foundation exam and beyond.* (2. izd.). IT Governance Publishing.
2. Butler, T. in O'Brien, L. (2019). Understanding regtech for digital regulatory compliance. V T. Lynn, J. Mooney, P. Rosati in M. Cummins (ur.), *Disrupting finance: fintech and strategy in the 21st century* (str. 85–102). Springer. https://doi.org/10.1007/978-3-030-02330-0_6
3. Hofstede, G., Hofstede, G. J. in Minkov, M. (2011). *Cultures and organizations: software of the mind* (3. izd.). McGraw-Hill.
4. Mohamed, H. in Yildirim, R. (2021). RegTech and regulatory change management for financial institutions. V A. Hamdan, A. E. Hassanien, A. Razzaque in B. Alareeni (ur.), *The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success* (str. 153–168). Springer.

5. Phillips, J. in Klein, J. D. (2022). Change management: From theory to practice. *TechTrends*, *67*(1), 189–197. https://doi.org/10.1007/s11528-022-00775-0

LITERATURA IN VIRI

1. Abdel-Hamid, T. in Madnick, S. E. (1991). *Software project dynamics: an integrated approach.* Prentice-Hall.
2. Abdullah, H. (2019). Analyzing the technological challenges of Governance, Risk and Compliance (GRC). V *2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)* (str. 274–282). IEEE.
3. Agencija za zavarovalni nadzor – AZN. (brez datuma a). *Ustanovitev in pravni položaj.* https://www.a-zn.si/o-agenciji/naloge-in-cilji/ustanovitev-pravni-polozaj/
4. Agencija za zavarovalni nadzor – AZN. (brez datuma b). *Naloge in pristojnosti.* https://www.a-zn.si/o-agenciji/naloge-in-cilji/naloge-in-pristojnosti/
5. Agencija za zavarovalni nadzor – AZN. (2020, 13. oktober). *Sporočilo za javnost: Uporaba sklepa "Decision of the Board of Supervisors on the cooperation of the competent authorities of the member states of the European Economic Area with regard to directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution".* https://www.a-zn.si/sporocilo-za-javnost-uporaba-sklepa-decision-board-supervisors-cooperation-competent-authorities-member-states-european-economic-area-regard-directive/
6. Agutter, C. (2020). *ITIL 4 essentials: your essential guide for the ITIL 4 foundation exam and beyond.* (2. izd.). IT Governance Publishing.
7. Anagnostopoulos, I. (2018). Fintech and regtech: impact on regulators and banks. *Journal of Economics and Business*, *100*, 7–25. https://doi.org/10.1016/j.jeconbus.2018.07.003
8. Anderson, D. in Anderson, L. A. (2002). *Beyond change management: advanced strategies for today's transformational leaders.* John Wiley & Sons.
9. Arner, D. W., Zetzsche, D. A., Buckley, R. P. in Barberis, J. N. (2017). Fintech and regtech: enabling innovation while preserving financial stability. *Georgetown Journal of International Affairs*, *18*(3), 47–58. https://www.jstor.org/stable/26395923
10. Aubert, B. A., Dussault, S., Patry, M. in Rivard, S. (1999). Managing the risk of IT outsourcing. V *Proceedings of the 32nd Annual Hawaii International Conference on System Sciences* (str. 1–11). IEEE.
11. Baker, M. in Hart, S. (2008). *The marketing book* (6. izd.). Routledge.
12. Beckett, P. (2017). GDPR compliance: your tech department's next big opportunity. *Computer Fraud & Security*, *2017*(5), 9–13. https://doi.org/10.1016/S1361-3723(17)30041-6
13. Belak, J. (2010). *Integralni management – MER model*. Založba MER, MER evrocenter.

14. Bélanger, F. in Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in IS. *MIS Quarterly*, *35*(4), 1017–1041. https://doi.org/10.2307/41409971
15. Bian, Y., Yang, C., Zhao, J. L. in Liang, L. (2018). Good drivers pay less: A study of usage-based vehicle insurance models. *Transportation Research Part A: Policy and Practice*, *107*, 20–34. https://doi.org/10.1016/j.tra.2017.10.018
16. Bijelić, M. (1998). *Zavarovanje in pozavarovanje.* Art Agencija.
17. Black, R. (2014). *Advanced software testing* (2. izd.). Rocky Nook.
18. Bolognini, L. in Bistolfi, C. (2017). Pseudonymization and impacts of big (personal/anonymous) data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review, 33*(2), 171–181. https://doi.org/10.1016/j.clsr.2016.11.002
19. Bowman, J. in Gufflet, M. (2017). Meeting the challenge of a global GDPR and BCR programme. *European Data Protection Law Review*, *3*(2), 257–266. https://doi.org/10.21552/edpl/2017/2/21
20. Brandtzaeg, P. B., Pultier, A. in Moen, G. M. (2019). Losing control to data-hungry apps: a mixed-methods approach to mobile app privacy. *Social Science Computer Review*, *37*(4), 466–488. https://doi.org/10.1177/0894439318777706
21. Butler, T. in O'Brien, L. (2019). Understanding regtech for digital regulatory compliance. V T. Lynn, J. Mooney, P. Rosati in M. Cummins (ur.), *Disrupting finance: fintech and strategy in the 21st century* (str. 85–102). Springer. https://doi.org/10.1007/978-3-030-02330-0_6
22. Cameron, E. in Green, M. (2019). *Making sense of change management: a complete guide to the models, tools and techniques of organizational change* (4. izd.). Kogan Page.
23. Custers, B., Dechesne, F., Sears, A. M., Tani, T. in van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, *34*(2), 234–243. https://doi.org/10.1016/j.clsr.2017.09.001
24. Cohen, S., Dori, D. in de Haan, U. (2010). A software system development life cycle model for improved stakeholders' communication and collaboration. *International Journal of Computers Communications & Control*, *5*(1), 20–41. https://doi.org/10.15837/ijccc.2010.1.2462
25. Ćirić, Z. in Raković, L. (2010). Change management in information system development and implementation projects. *Management Information Systems*, *5*(2), 23–28. https://doi.org/10.13140/RG.2.2.13973.27365
26. De Haes, S. in Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal*, *1*, 27–33. https://static.aminer.org/pdf/PDF/000/245/098/introduction_to_the_minitrack_it_governance_and_its_mechanisms.pdf

27. De Haes, S., Van Grembergen, W. in Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307–324. https://doi.org/10.2308/isys-50422
28. De la Cámara, M., Marcilla, F. J. S., Calvo-Manzano, J. A. in Fernández Vicente, E. (2012). Integrating governance, service management and project management of IT. V D. Winkler, R. V. O'Connor in R. Messnarz (ur.), *Systems, software and services process improvement* (str. 103–114). Springer. https://doi.org/10.1007/978-3-642-31199-4_10
29. Delovna skupina za varstvo podatkov iz člena 29. (2017). *Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je »verjetno, da bi obdelava povzročila veliko tveganje«, za namene Uredbe (EU) 2016/679.* https://www.ip-rs.si/fileadmin/user_upload/Pdf/Mednarodno_delovanje/wp248_rev.01_sl.pdf
30. Denham, E. (2017, 6. december). *Consent is not the 'silver bullet' for GDPR compliance.* https://digileaders.com/consent-not-silver-bullet-gdpr-compliance/
31. Djinović, M. (2018). Vse, kar morate vedeti o privolitvi za obdelavo osebnih podatkov. *Glas gospodarstva*, 4, 26–27. https://www.gzs.si/Portals/SN-informacije-Pomoc/Vsebine/GG/2018-april/26-27-GDPR.pdf
32. Dornberger, R., Inglese, T., Korkut, S. in Zhong, V. J. (2018). Digitalization: yesterday, today and tomorrow. V R. Dornberger (ur.), *Business information systems and technology 4.0* (str. 1–11). Springer.
33. European Banking Authority. (2021). *EBA analysis of RegTech in the EU financial sector.* https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf
34. European Insurance and Occupational Pensions Authority – EIOPA. (2017). *Draft implementing technical standards concerning a standardised presentation ofrmat for the Insurance Product Information Document of the Insurance Distribution Directive.* https://www.eiopa.europa.eu/document/download/2d4803d1-d75d-4ddb-91a1-cdce940696af_en?filename=Draft%20Implementing%20Technical%20Standards%20on%20the%20Insurance%20Product%20Information%20Document.pdf
35. European Parliament. (brez datuma). *2012/0011(COD): personal data protection: processing and free movement of data (General Data Protection Regulation).* https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2012/0011(COD)
36. European Union Agency for Network and Information Security – ENISA. (2018). *Recommendations on shaping technology according to GDPR provisions: exploring the notion of data protection by default.* https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O.2.2.5%20Recommendations%20on%20shaping%20technology%20according%20to%20GDPR%20provisions%20-%20Part%202.pdf

37. Evropska komisija. (brez datuma a). *Razlaga varstva podatkov.* https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en?prefLang=sl&etrans=sl
38. Evropska komisija. (brez datuma b). *Kdo je upravljavec in kdo obdelovalec podatkov?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_sl
39. Evropska komisija. (brez datuma c). *Kakšni so razlogi v zakonitem interesu?* https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_sl
40. Evropska unija. (brez datuma). *Vrste zakonodajnih aktov.* https://european-union.europa.eu/institutions-law-budget/law/types-legislation_sl
41. Falco, G. (2019). Participatory AI: reducing AI bias and developing socially responsible AI in smart cities. V *2019 IEEE International Conference on Computational Science and Engineering (CSE)* (str. 154–158). IEEE.
42. Financial Conduct Authority. (2018). *Insurance Distribution Directive Instrument 2018*. Financial Conduct Authority.
43. Freij, Å. (2018). A regulatory innovation framework: how regulatory change leads to innovation outcomes for fintechs. V R. Teigland, S. Siri, A. Larsson, A. M. Puertas in C. I. Bogusz (ur), *The rise and development of fintech: accounts of disruption from Sweden and beyond* (str. 21–42). Routledge.
44. Freij, Å. (2021). Regulatory change impact on technology and associated mitigation capabilities. *Technology Analysis & Strategic Management*, *34*(12), 1418–1431. https://doi.org/10.1080/09537325.2021.1963426
45. GRO Solutions. (2025, 21. november). *ISO 27001 and the GDPR.* https://www.itgovernance.co.uk/gdpr-and-iso-27001
46. Hiatt, J. (2006). *ADKAR: A model for change in business, government and our community.* Prosci Research.
47. Hodgson, L. (2018, 16. februar). *IDD delay approved by EU Council.* https://www.regulationtomorrow.com/eu/idd-delay-approved-by-eu-council/
48. Hofstede, G., Hofstede, G. J. in Minkov, M. (2011). *Cultures and organizations: software of the mind* (3. izd.). McGraw-Hill.
49. Horák, M., Stupka, V. in Husák, M. (2019). GDPR compliance in cybersecurity software: A case study of DPIA in an information sharing platform. V *Proceedings of the 14th International Conference on Availability, Reliability and Security* (str. 1–8). Association for Computing Machinery.
50. Iden, J. in Eikebrokk, T. R. (2013). Implementing IT service management: A systematic literature review. *International Journal of Information Management*, *33*(3), 512–523. https://doi.org/10.1016/j.ijinfomgt.2013.01.004

51. Informacijski pooblaščenec Republike Slovenije. (2015). *Zavarovanje osebnih podatkov: smernice informacijskega pooblaščenca.* https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_zavarovanju_OP.pdf
52. Informacijski pooblaščenec Republike Slovenije. (brez datuma a). *Varnost osebnih podatkov.* https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/zavarovanje-oz-varnost-osebnih-podatkov
53. Informacijski pooblaščenec Republike Slovenije. (brez datuma b). *Varstvo osebnih podatkov na internetu.* https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/
54. Informacijski pooblaščenec Republike Slovenije. (brez datuma c). *Varstvo osebnih podatkov.* https://www.ip-rs.si/o-pooblascencu/pristojnosti/varstvo-osebnih-podatkov
55. Informacijski pooblaščenec Republike Slovenije. (brez datuma č). *Pravne podlage – zasebni sektor s pogoji privolitve [infografika].* https://www.ip-rs.si/fileadmin/user_upload/png/infografike/pravne_podlage_zasebni_sektor_s_pogoji_privolitve_01.png
56. Informacijski pooblaščenec Republike Slovenije. (brez datuma d). *Seznanitev z lastnimi osebnimi podatki ali pravica do dostopa do osebnih podatkov.* https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/seznanitev-z-lastnimi-osebnimi-podatki
57. Informacijski pooblaščenec Republike Slovenije. (brez datuma e). *Najpogostejša vprašanja in odgovori.* https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/najpogostejsa-vprasanja-in-odgovori
58. International Organization for Standardization – ISO. (2011a). *ISO/IEC 27005:2011 — Information technology — Security techniques — Information security risk management.* ISO.
59. International Organization for Standardization – ISO. (2011b). *ISO/IEC 29100 — Privacy framework.* ISO.
60. International Organization for Standardization – ISO. (2013). *ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.* ISO.
61. International Organization for Standardization – ISO. (2018). *ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary.* ISO.
62. International Organization for Standardization – ISO. (2019a). *ISO/IEC 27018:2019 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.* ISO.
63. International Organization for Standardization – ISO. (2019b). *ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/UEC 27002 for privacy information management – requirements and guidelines.* ISO.

64. International Organization for Standardization – ISO. (2025). *ISO/IEC 27701:2025: Information security, cybersecurity and privacy protection – Privacy information management systems – Recuirements and guidance*. ISO.
65. IT Governance Institute. (2003). *Board briefing on IT governance* (2. izd.). IT Governance institute. https://web.archive.org/web/20150506091126/http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf
66. Jurison, J. (1999). Software project management: the manager's view. *Communications of the Association for Information Systems*, *2*(1), 1–58. https://doi.org/10.17705/1CAIS.00217
67. Karadzhov, V. in Patarchanova, E. (2025). How to create the best PESTEL analysis. *International Journal of Digital Research*, *1*(3), 8–20. https://doi.org/10.63711/ijdr.net20250301
68. Karczewska, J. (2017, 24. maj). *COBIT 5 and the GDPR*. https://www.isaca.org/resources/news-and-trends/industry-news/2017/cobit-5-and-the-gdpr
69. Ko, D. in Fink, D. (2010). Information technology governance: an evaluation of the theory–practice gap. *Corporate Governance*, *10*(5), 662–674. https://doi.org/10.1108/14720701011085616
70. Kotter, J. P. (2012). Accelerate! *Harvard Business Review*, *90*(11), 44–58.
71. Krajnc, T. (2005). ITIL – upravljanje IT storitev. *Organizacija, 38*(6), 302–308.
72. Krumberger, M. (2015). Zavarovalništvo kot pomembna gospodarska panoga. *Podjetje in delo*, *41*(6/7), 1010–1027. http://dlib.si/details/URN:NBN:SI:DOC-B4FG0Q4H
73. Lehmann, V. (2010). Connecting changes to projects using a historical perspective: Towards some new canvases for researchers. *International Journal of Project Management*, *28*(4), 328–338. https://doi.org/10.1016/j.ijproman.2010.01.011
74. Lehtonen, T.-K. in Liukko, J. (2012). The forms and limits of insurance solidarity. *Journal of Business Ethics, 103*(S1), 33–44. https://doi.org/10.1007/s10551-012-1221-x
75. Lombardi, R., Del Giudice, M., Caputo, A., Evangelista, F. in Russo, G. (2016). Governance and assessment insights in information technology: The Val IT model. *Journal of the Knowledge Economy*, *7*(1), 292–308. https://doi.org/10.1007/s13132-015-0328-6
76. Luo, L. (2001). *Software testing techniques.* Carnegie Mellon University.
77. Malinowska, K. (2016). Insurance transparency and protection regime under the Insurance Distribution Directive. *Insurance Review,* 4, 89–101. https://piu.org.pl/wp-content/uploads/2017/05/WU-2016-04-06-Malinowska-en.pdf
78. Mani, Z. in Chouk, I. (2019). Impact of privacy concerns on resistance to smart services: Does the "big brother effect" matter? *Journal of Marketing Management*, *35*(15–16), 1460–1479. https://doi.org/10.1080/0267257X.2019.1667856
79. Miguéis, V. L., Camanho, A. S. in Falcão e Cunha, J. F. (2012). Customer data mining for lifestyle segmentation. *Expert Systems with Applications*, *39*(10), 9359–9366. https://doi.org/10.1016/j.eswa.2012.02.133

80. Miller, K. (2020, 19. marec). *5 critical steps in the change management process* [objava na blogu]. https://online.hbs.edu/blog/post/change-management-process
81. Mohamed, H. in Yildirim, R. (2021). RegTech and regulatory change management for financial institutions. V A. Hamdan, A. E. Hassanien, A. Razzaque in B. Alareeni (ur.), *The Fourth industrial revolution: implementation of Artificial Intelligence for growing business success* (str. 153–168). Springer.
82. Morey, T., Forbath, T. in Schoop, A. (2015). Customer data: designing for transparency and trust. *Harvard Business Review*, *93*(5), 96–105.
83. Murthy, S., Bakar, A. A., Rahim, F. A. in Ramli, R. (2019). A comparative study of data anonymization techniques. V *2019 IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity), High performance and Smart Computing (HPSC) and Intelligent Data and Security (IDS)* (str. 306–309). IEEE.
84. Nekrep, M. (2018). Ponudba zavarovalnih storitev v obdobju digitalizacije. *Zavarovalniški horizonti*, *14*(6), 5–17.
85. Overby, E., Bharadwaj, A. in Sambamurthy, V. (2006). Enterprise agility and the enabling role of information technology. *European Journal of Information Systems*, *15*(2), 120–131. https://doi.org/10.1057/palgrave.ejis.3000600
86. Pasquini, A. in Galiè, E. (2013). COBIT 5 and the process capability model: Improvements provided for IT governance process. V P. Michelberger (ur.), *Proceedings of FIKUSZ* '13, (str. 67–76). Obuda University, Kelet Faculty of Business and Management.
87. Phillips, J. in Klein, J. D. (2022). Change management: from theory to practice. *TechTrends*, *67*(1), 189–197. https://doi.org/10.1007/s11528-022-00775-0
88. Pilič, I. in Agafonova, J. (2017). Sodobne prodajne poti v zavarovalništvu: revolucija ali evolucija? V *Moderne prodajne poti v zavarovalništvu* (str. 11–19). Slovensko zavarovalno združenje.
89. Pirc Musar & partnerji. (2017, 4. julij). *GDPR bo jutri tu, ste pripravljeni?* https://pirc-musar.si/gdpr-varstvo-osebnih-podatkov/
90. Politou, E., Alepis, E. in Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), 1–20. https://doi.org/10.1093/cybsec/tyy001
91. Politou, E., Michota, A., Alepis, E., Pocs, M. in Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: an uneasy relationship. *Computer Law & Security Review*, *34*(6), 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006
92. Pollack, J. in Algeo, C. (2014). Perspectives on the formal authority between project managers and change managers. *Project Management Journal*, *45*(5), 27–43. https://doi.org/10.1002/pmj.21446
93. Project Management Institute. (2021). *A guide to the project management body of knowledge (PMBOK® Guide)*(7. izd.). Project Management Institute.

94. Racz, N., Weippl, E. in Seufert, A. (2010). A frame of reference for research of integrated governance, risk and compliance (GRC). V B. De Decker in I. Schaumüller-Bichl (ur.), *IFIP International Conference on Communications and Multimedia Security* (str. 106–117). Springer.
95. Reiter, M. in Miklosík, A. (2020). Digital transformation of organisations in the context of ITIL® 4. *Marketing Identity, 8*(1), 522–536.
96. Richter, H. in Lantow, B. (2022). IT-service value modeling: a systematic literature analysis. V W. Abramowicz, S. Auer in M. Strozyna (ur.), *International Conference on Business Information Systems* (str. 267–278). Springer.
97. Robinson, N. (2005). IT excellence starts with governance. *Journal of Investment Compliance*, *6*(3), 45–49. https://doi.org/10.1108/15285810510659310
98. Ryan, P., Crane, M. in Brennan, R. (2021). GDPR compliance tools: Best practice from RegTech. V J. Filipe, M. Śmiałek, A. Brodsky in S. Hammoudi (ur.), *Enterprise Information Systems: 22nd International Conference, ICEIS 2020* (str. 905–929). Springer.
99. Sallé, M. (2004). *IT service management and IT governance: review, comparative analysis and their impact on utility computing*. http://shiftleft.com/mirrors/www.hpl.hp.com/techreports/2004/HPL-2004-98.pdf
100. Sköld, M., Freij, Å. in Frishammar, J. (2020). New entrant or incumbent advantage in light of regulatory change: a multiple case study of the Swedish life insurance industry. *European Management Review*, *17*(1), 209–227. https://doi.org/10.1111/emre.12345
101. Slovensko zavarovalno združenje. (2018, 26. september). *Nova pravila prodaje zavarovanj*. https://www.zav-zdruzenje.si/2018/09/26/v-veljavo-stopajo-nova-pravila-prodaje-zavarovanj/
102. Soumelidou, A. in Tsohou, A. (2021). Towards the creation of a profile of the information privacy aware user: a systematic literature review. *Telematics and Informatics*, 61. https://doi.org/10.1016/j.tele.2021.101592
103. Splošna uredba EU o varstvu podatkov – GDPR. *Uradni list EU, L 119.*
104. Stoneburner, G., Goguen, A. in Feringa, A. (2002). *Risk management guide for information technology systems (NIST SP 800-30).* National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01
105. Tallon, P. P. in Pinsonneault, A. (2011). Competing perspectives on the link between strategic information technology alignment and organizational agility. *MIS Quarterly, 35*(2), 463–486. https://doi.org/10.2307/23044052
106. Tavani, H. T. (1999). Informational privacy, data mining, and the internet. *Ethics and Information Technology*, *1*(2), 137–145. https://doi.org/10.1023/A:1010063528863
107. Tikkinen-Piri, C., Rohunen, A. in Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

108. Trinkaus, Z. in Pahor, M. (2017). Slovenski poskus št. 1 oziroma prvi osnutek novele Zakona o varstvu osebnih podatkov. *Pravna praksa, 36*(43)*,* 23–25.
109. Uradni list Republike Slovenije. (2023, 5. april). *ZVOP-2 je začel veljati 26. januarja 2023 – kakšne pomembne novosti prinaša?* https://www.uradni-list.si/novice/pogled/zvop-2-je-zacel-veljati-26--januarja-2023---kaksne-pomembne-novosti-prinasa
110. Van Deursen, S. in Kummeling, H. (2019). The New Silk Road: a bumpy ride for Sino-European collaborative research under the GDPR? *Higher Education*, *78*(5), 911–930. https://doi.org/10.1007/s10734-019-00377-5
111. Varajão, J., Fernandes, G. in Silva, H. (2020). Most used project management tools and techniques in information systems projects. *Journal of Systems and Information Technology*, *22*(3), 225–242. https://doi.org/10.1108/JSIT-08-2017-0070
112. Vidonja, W. (2016). Distribucija zavarovanj: nova evropska direktivna pokrajina. V *Osrednji temi Moderne prodajne poti v zavarovalništvu, Zavarovalništvo – partner države ali država – partner zavarovalništva: e-zbornik* (str. 27–32). Slovensko zavarovalno združenje.
113. White, S. K. (2023, 12. junij). What is COBIT? A framework for alignment and governance. *CIO Magazine*. https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html
114. Wu, S. P.-J., Straub, D. W. in Liang, T. P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance. *MIS Quarterly*, *39*(2), 497–518. https://doi.org/10.25300/MISQ/2015/39.2.10
115. Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu (ZZavar-1A). *Uradni list RS, št. 9/19*.
116. Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu (ZZavar-1B). *Uradni list RS, št. 102/2020*.
117. Zakon o spremembah in dopolnitvah Zakona o zavarovalništvu (ZZavar-1D). *Uradni list RS, št. 77/2025.*
118. Zakon o varstvu osebnih podatkov (ZVOP-1). *Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 177/20 – ZVOPOKD in 163/22 – ZVOP-2.*
119. Zakon o varstvu osebnih podatkov (ZVOP-2). *Uradni list RS, št. 163/22 in 40/25 – ZInfV-1*.
120. Zakon o zavarovalništvu (ZZavar-1)*. Uradni list RS, št. 93/15, 9/19, 102/20, 48/23, 78/23 – ZZVZZ-T, 84/24 – odl. US in 77/25*.
121. Zasa, F. P., Patrucco, A. in Pellizzoni, E. (2020). Managing the hybrid organization: how can agile and traditional project management coexist? *Research-Technology Management*, *64*(1), 54–63. https://doi.org/10.1080/08956308.2021.1843331

122. Zavarovalnica Triglav, d. d. (2024). *Letno poročilo Skupine Triglav in Zavarovalnice Triglav, d. d., 2023.* https://letnoporocilo.triglav.eu/storage/doc/202403/letno-porocilo-skupine-in-zavarovalnice-triglav-2023.pdf
123. Zerlang, J. (2017). GDPR: a milestone in convergence for cybersecurity and compliance. *Network Security*, *2017*(6), 8–11. https://doi.org/10.1016/S1353-4858(17)30060-0