UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA SKLADNOSTI DELA RAČUNOVODSKIH SERVISOV Z ZAKONODAJO O VARSTVU OSEBNIH PODATKOV

Ljubljana, april 2026 MANCA STANIŠA

IZJAVA O AVTORSTVU

Podpisana Manca Staniša, študentka Univerze v Ljubljani Ekonomske fakultete, avtorica predloženega dela z naslovom Analiza skladnosti dela računovodskih servisov z zakonodajo o varstvu osebnih podatkov, pripravljenega v sodelovanju z mentorico doc. dr. Ano Čertanec

I Z J A V L J A M

1. da sem predloženo delo pripravila 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 poskrbela, 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 Univerze v Ljubljani Ekonomski fakulteti v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila 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 preverila verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne 10. 04. 2026 Podpis študentke: Manca Staniša

POVZETEK

Magistrsko delo obravnava skladnost delovanja manjših računovodskih servisov z zakonodajo na področju varstva osebnih podatkov v Sloveniji, zlasti v okviru GDPR in ZVOP-2. Namen raziskave je bil analizirati, v kolikšni meri so manjši računovodski servisi svoje poslovanje prilagodili zakonskim zahtevam in kako se te odražajo v njihovih delovnih procesih. Teoretični del temelji na pregledu domače in tuje literature ter zakonodajnega okvira, praktični del pa na kvalitativni raziskavi, izvedeni z globinskimi intervjuji v manjših računovodskih servisih. Rezultati analize kažejo, da manjši računovodski servisi večinoma odgovorno izvajajo osnovne tehnične in organizacijske ukrepe za varovanje osebnih podatkov, vendar se stopnja skladnosti med posameznimi servisi razlikuje. Poleg tega večina intervjuvanih manjših računovodskih servisov nima urejene predpisane dokumentacije na področju varstva osebnih podatkov.

KLJUČNE BESEDE: GDPR, računovodstvo, manjši računovodski servisi, osebni podatki, varstvo osebnih podatkov

CILJI TRAJNOSTNEGA RAZVOJA



ABSTRACT

The master's thesis examines the compliance of small accounting service providers with personal data protection legalisation in Slovenia, particularly within the framework of the GDPR and ZVOP-2. The aim of the research was to analyse the extent to which small accounting service providers have adapted their operations to legal requirements and how these requirements are reflected in their work processes. The theoretical part is based on a review of domestic and foreign literature as well as the relevant legislative framework, while the empirical part is grounded in qualitative research conducted through in-depth interviews with small accounting service providers. The results of the analysis indicate that small accounting service providers generally implement basic technical and organizational measures for the protection of personal data in responsible manner, however, the level o compliance varies among individual providers. Furthermore, most of the interviewed small accounting service providers do not have the prescribed documentation in the field of personal data protection properly arranged.

KEY WORDS: GDPR, accounting, small accounting service providers, personal data, personal data protection

SUSTAINABLE DEVELOPMENT GOALS



KAZALO

1 UVOD 1

2 RAČUNOVODSTVO 3

2.1 Vrste računovodstev 5

2.2 Računovodski izkazi 6

2.3 Zakonska podlaga in strokovni okvirji računovodstva v Sloveniji 7

2.3.1 Zakon o gospodarskih družbah 7

2.3.2 Slovenski računovodski standardi 8

2.3.3 Zakon o računovodstvu 8

2.3.4 Mednarodni standardi računovodskega poročanja 9

2.4 Računovodski servisi 10

2.4.1 Računovodstvo kot poklic 11

3 ZAKONSKA PODLAGA VARSTVA OSEBNIH PODATKOV V SLOVENIJI 12

3.1 Splošna uredba o varstvu osebnih podatkov 12

3.1.1 Pravni okvir obdelave osebnih podatkov po splošni uredbi 13

3.1.2 Pravice posameznika, na katerega se nanašajo osebni podatki 14

3.1.3 Neodvisni nadzorni organ in pooblaščena oseba za varstvo podatkov 16

3.1.4 Ključni dokumenti 17

3.2 Zakon o varstvu osebnih podatkov 19

3.2.1 Zagotavljanje varstva osebnih podatkov 20

3.2.2 Videonadzor ter evidentiranje vstopov in izstopov iz službenih prostorov. 21

3.2.3 Obdelava biometričnih in genskih podatkov 22

3.2.4 Kazenske določbe 22

3.3 Informacijski pooblaščenec 23

4 VARSTVO OSEBNIH PODATKOV V RAČUNOVODSTVU 23

4.1 Obdelava osebnih podatkov v računovodstvu 24

4.1.1 Hramba in evidenca obdelave osebnih podatkov 26

4.1.2 Zagotovitev tehničnih in organizacijskih ukrepov za zaščito osebnih podatkov 26

4.1.3 Pogodbeno razmerje med upravljavcem in obdelovalcem 27

4.1.4 Obdelava osebnih podatkov pri računovodstvu v oblaku 28

4.2 Izzivi, prednosti in uporaba splošne uredbe v računovodstvu 28

4.2.1 Uporabnost, izzivi in prednosti uvedbe zahtev splošne uredbe v manjših podjetjih ... 29
4.3 Zakon o preprečevanju pranja denarja in financiranja terorizma v računovodstvu ter varstvo osebnih podatkov ... 31
5 EMPIRIČNI DEL ... 32
5.1 Analiza globinskih intervjujev po tematskih sklopih ... 34
5.1.1 Poznavanje zakonodaje ... 34
5.1.2 Notranja politika v računovodskem servisu ... 36
5.1.3 Pogodbena ureditev s strankami ... 40
5.1.4 Tehnični in organizacijski ukrepi ... 42
5.1.5 Skladnost z zakonodajo v praksi ... 45
5.1.6 Izzivi ... 47
5.1.7 Vpliv zakonodaje ... 50
5.2 Ugotovitve intervjujev in diskusija ... 52
6 SKLEP ... 53
SEZNAM KLJUČNE LITERATURE ... 57
LITERATURA IN VIRI ... 57
PRILOGE ... 62

KAZALO TABEL

Tabela 1: Poznavanje zakonodaje ... 34
Tabela 2: Notranja politika v računovodskem servisu ... 36
Tabela 3: Pogodbena ureditev s strankami ... 40
Tabela 4: Tehnični in organizacijski ukrepi ... 43
Tabela 5: Skladnost z zakonodajo v praksi ... 45
Tabela 6: Izzivi ... 48
Tabela 7: Vpliv zakonodaje ... 51

KAZALO SLIK

Slika 1: Ključne obveznosti računovodskih servisov ... 35
Slika 2: Vrste obdelovanih osebnih podatkov ... 38
Slika 3: Glavni izzivi ... 49
Slika 4: Največja tveganja ... 50

KAZALO PRILOG

Priloga 1: Okvirna vprašanja za lastnike/zastopnike računovodskih servisov 1
Priloga 2: Informacije o izvedbi intervjujev z lastniki/zastopniki računovodskih servisov .. 3
Priloga 3: Transkript intervjuja INT1 4
Priloga 4: Transkript intervjuja INT2 10
Priloga 5: Transkript intervjuja INT3 15
Priloga 6: Transkript intervjuja INT4 20
Priloga 7: Transkript intervjuja INT5 26
Priloga 8: Transkript intervjuja INT6 32
Priloga 9: Transkript intervjuja INT7 38
Priloga 10: Transkript intervjuja INT8 43

SEZNAM KRATIC

Angl. – angleško
AJPES – Agencija Republike Slovenije za javnopravne evidence in storitve
DDV – Davek na dodano vrednost
EGP – Evropski gospodarski prostor
EGS – Evropska gospodarska skupnost
ES – Evropski svet
EU – Evropska unija
GDPR – (angl. General data protection regulation); Splošna uredba o varstvu podatkov
IPRS – Informacijski pooblaščenec Republike Slovenije
IP – Internetni protokol
IT – Informacijska tehnologija
MAC – (angl. Media Access Control); Naslov za nadzor dostopa do medija
MRS – Mednarodni računovodski standardi
MSRP – Mednarodni standardi računovodskega poročanja
PSR – Pravila skrbnega računovodenja
SRKRD – Sekcija podjetij računovodskih, knjigovodskih, revizijskih in davčno svetovalnih storitev
SRS – Slovenski računovodski standardi
ZDru-1 – Zakon o društvih
ZGD-1 – Zakon o gospodarskih družbah
ZGJS – Zakon o javnih službah
ZInfP – Zakon o informacijskem pooblaščencu
ZJF – Zakon o javnih financah
ZPPDFT-2 – Zakon o preprečevanju pranja denarja in financiranja terorizma

ZR – Zakon o računovodstvu
ZRS – Združenje računovodskih servisov
ZRFR – Zveza računovodij, finančnikov in revizorjev Slovenije
ZVOPOKD – Zakon o varstvu osebnih podatkov na področju kaznivih dejanj

1 UVOD

Področje varstva osebnih podatkov je v Sloveniji najprej urejal Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 177/20 in 163/22 – ZVOP-2. Leta 2018 ga je dopolnila Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju Splošna uredba o varstvu podatkov ali GDPR, Uradni list EU, št. L119/1), ki velja na področju celotne Evropske unije. Na začetku leta 2023 je v veljavo stopil Zakon o varstvu osebnih podatkov (ZVOP-2) Uradni list RS, št. 163/22, pri čemer je ZVOP-1 prenehal veljati. Čeprav zakonodaja s področja varstva osebnih podatkov zajema širše področje, se v svojem magistrskem delu osredotočam na njeno vlogo in vpliv v manjših računovodskih servisih.

Računovodski servisi so odgovorni za varovanje številnih pomembnih podatkov, med drugim tudi osebnih (Bajuk Mušič, 2018). Obdelava osebnih podatkov zajema širok spekter dejavnosti, ki se lahko izvajajo ročno ali avtomatizirano. To vključuje zbiranje, snemanje, organiziranje, strukturiranje, shranjevanje, prilagoditev ali spremembo, priklic, posvetovanje, uporabo, razkritje s prenosom, razširjanje ali drugačno dajanje na voljo, poravnavo ali kombinacijo, omejitev, izbris ali uničenje (4. člen GDPR). Primeri obdelave podatkov so upravljanje kadrov in obračunavanje plač, dostop do zbirke podatkov o stikih, ki vsebujejo osebne podatke, pošiljanje promocijske elektronske pošte, razrez dokumentov, ki vsebujejo osebne podatke, pošiljanje ali objavljanje fotografije osebe na spletnem mestu, shranjevanje naslovov IP ali MAC in videonadzore (European Commission, 2025). Zaradi narave svojega dela so računovodski servisi pogodbeni obdelovalec podatkov, njegove obveznosti pa določata GRPR in ZVOP-2 (Informacijski pooblaščenec, 2024a). Za obdelavo osebnih podatkov mora obstajati pravna podlaga, in sicer gre lahko za privolitev, pogodbo, zakonsko obveznost, življenjske interese, izvajanje javne naloge ali zakonite interese. Računovodski servis obdeluje osebne podatke na podlagi izpolnjevanja zakonskih obveznosti in pogodb, ki jih sklene s stranko. Pogodba kot pravna podlaga za obdelavo osebnih podatkov nastane takrat, ko se med posameznikom in obdelovalcem podatkov podpiše pogodba ali kadar se izvajajo ukrepi na zahtevo tega posameznika pred sklenitvijo pogodbe (Informacijski pooblaščenec, 2024b).

Osebni podatki, ki jih obdeluje računovodstvo, so v prvi vrsti, z vidika računovodskega servisa kot delodajalca, podatki o zaposlenih (Informacijski pooblaščenec, 2019). Kot pogodbeni obdelovalec podatkov se računovodski servis srečuje z osebnimi podatki kadrovskih evidenc in drugimi osebnimi podatki, potrebnimi za odtegljaje, obračune plač, davkov in prispevkov. Sem sodijo tudi avtorske pogodbe, podjemne pogodbe, pogodbe o občasnem delu upokojencev, štipendije, študentsko delo in podobo (Bajuk Mušič, 2018). Prav tako se srečuje z osebnimi podatki na izdanih računih fizičnim osebam kot kupcem (Informacijski pooblaščenec, 2019).

Zakonodaja o varstvu osebnih podatkov prinaša izboljšanje pravic in varnosti za posameznike, na katere se podatki nanašajo, vendar hkrati postavlja dodatne zahteve podjetjem, kar se odraža v povečanem obsegu dela in višjih stroških. Nanje lahko vpliva zagotavljanje ustreznega izobraževanja zaposlenih glede varovanja osebnih podatkov, kar lahko zahteva dodatne izvedbe usposabljanj in seminarjev. V večjih podjetjih se lahko celo pojavi potreba po dodatnem kadru. Vedno izrazitejša digitalizacija postopoma nadomešča papirno poslovanje z elektronskim, kar vpliva tudi na računovodske servise in shranjevanje njihovih podatkov. Potrebujejo namreč primerno programsko opremo za varno shranjevanje in obdelavo osebnih podatkov. To lahko prinese dodatne stroške za nakup, vzdrževanje in posodabljanje programske opreme ter vzpostavitev varnostnega sistema (Grgič, 2017). Razvoj in uveljavljanje politik zasebnosti in postopkov varovanja osebnih podatkov zahteva čas in sredstva, vključno s pravnimi strokovnjaki za skladnost s predpisi. Potrebni sta stalno spremljanje in posodabljanje postopkov v skladu z zakonodajo in regulativami v izogib potencialnim kaznim. V magistrskem delu preverjam, do kakšne mere je delo v manjših računovodskih servisih skladno z zakonodajo o varstvu osebnih podatkov. Posebna pozornost je namenjena temu, kako so servisi prilagodili svoje poslovanje zakonskim zahtevam na tem področju, ravnanju z osebnimi podatki in zagotavljanju predpisane dokumentacije.

Namen magistrskega dela je analizirati usklajenost delovanja manjših računovodskih servisov z zakonodajo na področju varstva osebnih podatkov. S celovitim pristopom raziskava razkriva kompleksno dinamiko, ki jo prinašajo zakonski okviri glede ravnanja z osebnimi podatki in njihovega varovanja v manjših računovodskih servisih. Z izvedbo poglobljenih intervjujev sem pridobila informacije in preučila, kako učinkovito so podjetja v praksi prilagodila svoje delo zahtevam zakonodaje.

Cilji magistrskega dela so:

1. opraviti temeljito analizo domače in tuje literature na področju varstva osebnih podatkov v računovodstvu, s poudarkom na identifikaciji ključnih konceptov, zakonskih predpisov in praks, ki zadevajo obravnavano tematiko. Z obsežnim pregledom literature delo zagotavlja trdno teoretično podlago za nadaljnje raziskovanje;
2. izvesti poglobljene intervjuje s pomočjo strukturiranih vprašalnikov za pridobitev obsežnih in kakovostnih podatkov o delovanju manjših računovodskih servisov ter njihovi skladnosti z zakonodajo o varstvu osebnih podatkov, ki bodo služili kot osnova za nadaljnjo analizo.
3. podrobno analizirati skladnost delovanja manjših računovodskih servisov z veljavno zakonodajo na področju varstva osebnih podatkov.

Osnovna teza magistrskega dela je:

Manjši računovodski servisi ustrezno ravnajo z osebnimi podatki svojih strank, vendar številni med njimi ne izpolnjujejo zahtev s področja zakonodaje o varstvu osebnih podatkov po izdelavi in vzdrževanju predpisane dokumentacije.

Raziskovalna vprašanja magistrskega dela so:

1. Kakšne obveznosti predpisuje trenutna zakonodaja s področja varstva osebnih podatkov računovodskim servisom?
2. Kako se predpisi s področja varstva osebnih podatkov odražajo v delovnih procesih manjših računovodskih servisov?
3. Kakšne so posledice zahtev, ki jih prinaša skladnost z zakonodajo o varstvu osebnih podatkov za manjše računovodske servise?
4. Katere so najpogostejše pomanjkljivosti v skladnosti dela manjših računovodskih servisov z zakonodajo s področja varstva osebnih podatkov?
5. Ali so delovni procesi manjših računovodskih servisov v skladu z zakonodajo varstva osebnih podatkov?

Magistrsko delo je strukturirano v dveh glavnih delih, ki zajemata teoretični in empirični del. V teoretičnem delu sistematično pregledam obstoječo domačo in mednarodno znanstveno literaturo, s poudarkom na tematiki varstva osebnih podatkov v kontekstu računovodstva. Pri tem uporabim opisno metodo raziskovanja, ki obsega več korakov, vključno z opisovanjem, opazovanjem, s primerjanjem, z analizo in s sklepanjem povezav. Osredotočam se na opis ključnih konceptov, zakonodajnih okvirov in praks, povezanih z varstvom osebnih podatkov v računovodskem okolju. Analiziram tudi vpliv relevantnih predpisov, kot sta GDPR in ZVOP-2, na računovodska podjetja ter njihovo delo. Raziskovalni del magistrskega dela je zasnovan kot empirična študija, ki temelji na kvalitativnih podatkih, pridobljenih z osmimi globinskimi intervjuji. Izvedla sem intervjuje v osmih manjših računovodskih podjetjih, pri čemer sem uporabila strukturiran vprašalnik, zasnovan z namenom pridobitve podatkov o skladnosti dela manjših računovodskih servisov z zakonodajo o varstvu osebnih podatkov. Raziskala sem, kako dobro so podjetja prilagodila svoje delo zahtevam zakona, ali ustrezno ravnajo z osebnimi podatki in ali imajo ustrezno dokumentacijo v skladu z zakonskimi predpisi. Skupaj teoretični in raziskovalni del magistrskega dela omogočata celovit vpogled v kompleksno tematiko varstva osebnih podatkov v računovodstvu ter ponudita ugotovitve in smernice za prakso in nadaljnje raziskave na tem področju.

2 RAČUNOVODSTVO

Beaver (2023) poudarja, da ima računovodstvo dolgo tradicijo, saj se je razvilo že v času prvih civilizacij, ki so začele beležiti menjavo dobrin. Današnji temelji izhajajo iz srednjega veka, ko je bilo razvito dvostavno knjigovodstvo, ki se uporablja še danes (Beaver, 2023). Računovodstvo najpogosteje razlagamo kot sistem beleženja, obdelave in poročanja o

poslovnih dogodkih. Gre za temeljno dejavnost, ki omogoča spremljanje finančnega dogajanja v podjetju ter zagotavlja informacije za sprejemanje odločitev in izpolnjevanje zakonskih obveznosti (Mayr, 2017). Računovodstvo uporabljajo vse družbe, ne glede na velikost, saj omogoča pravno skladnost in ocenjevanje finančnega zdravja poslovanja. Tobin (2025) poudarja, da osnovno poznavanje računovodskih pojmov ni koristno le za strokovnjake, temveč tudi za lastnike manjših družb in posameznike, ki lahko z njim pridobijo boljši vpogled v lastne finance. Računovodstvo namreč krepi finančno pismenost ter omogoča natančne in zanesljive informacije o finančnem stanju (Tobin, 2025).

Čeprav računovodstvo pogosto povezujemo zgolj s številkami in preglednicami, Beaver (2023) meni, da ima danes veliko širšo vlogo. Računovodje namreč s svojimi analizami prispevajo k oblikovanju poslovne strategije in sodelujejo z različnimi deležniki – od vodstva in investitorjev do oddelkov prodaje, kadrov in informatike. Poleg tega poudarja, da delujejo kot vez med podjetjem ter državnimi, davčnimi in regulatornimi organi. V praksi računovodstvo družbi omogoča pripravo ključnih poročil, kot so bilanca stanja, izkaz poslovnega izida, denarnih tokov in gibanja kapitala. Na podlagi teh informacij lahko vodstvo ocenjuje stroške dela, upravlja zaloge, prepoznava nove poslovne priložnosti, povečuje dobičkonosnost, nadzoruje denarni tok in spremlja splošno finančno zdravje podjetja. Podatki, ki jih pripravi računovodstvo, niso pomembni zgolj za interno uporabo, ampak so nujni tudi za banke, investitorje, revizorje in davčne organe.

Uporabnike računovodskih informacij se deli na zunanje in notranje. Zunanji uporabniki vključujejo lastnike brez dejavne vloge pri upravljanju podjetja, potencialne vlagatelje, posojilodajalce, dobavitelje, kupce, konkurente, državo in širšo zainteresirano javnost. Notranji uporabniki so poslovodstvo, lastniki z aktivno pravico odločanja in zaposleni. Nadaljuje, da mora računovodski informacijski sistem v prvi vrsti zagotoviti relevantne in pravočasne informacije za notranje uporabnike, saj s pomočjo teh podatkov sprejemajo ključne odločitve, ki vplivajo na uspešnost podjetja. Obseg in vsebina informacij, ki jih prejemajo zunanji uporabniki, sta določena z zakonskimi zahtevami, računovodskimi standardi in interesom podjetja za transparentno poslovanje (Igličar in drugi, 2017).

Igličar in drugi (2017) knjigovodstvo opredelijo kot del računovodstva, ki se ukvarja s spremljanjem podatkov preteklega poslovanja podjetja. Zajema podatke vseh gospodarskih kategorij, ki so izraženi v denarni merski enoti. Menijo, da ga lahko opredelimo kot posebno vrsto evidentiranja poslovanja, v sklopu katerega sistematično zbiramo, urejamo, obdelujemo in shranjujemo knjigovodske podatke in informacije o poslovanju ter jih nato posredujemo določenim uporabnikom v obliki knjigovodskih poročil. Poznavanje podatkov o preteklem poslovanju podjetja je pomembno za uspešno poslovanje. Trdijo, da na eni strani daje informacije, ki so podlaga za uspešno vodenje in upravljanje podjetja, na drugi strani pa knjigovodstvo evidentira izhodiščne podatke za ostale tri računovodske funkcije – to so računovodsko predračunavanje, računovodsko nadziranje in računovodsko analiziranje. Knjigovodstvo v sklopu računovodstva neposredno zajema vse spremembe, ki se nanašajo na sredstva, obveznosti do virov sredstev, stroške, prihodke, odhodke in poslovni izid.

Posredno knjigovodstvo spremlja tudi prejemke in izdatke oziroma denarne tokove (Igličar in drugi, 2017).

Delo računovodij je raznoliko in vključuje preglede finančnih informacij, analizo računov, pripravo poračunov in poročil ter svetovanje glede finančnega poslovanja. V manjših družbah računovodje pogosto opravljajo tudi naloge knjigovodstva, kot so vodenje glavne knjige, obračun plač, plačevanje računov in usklajevanje evidenc. V večjih družbah računovodski strokovnjaki sodelujejo v širših ekipah, ki skrbijo za celovito finančno upravljanje družbe (Beaver, 2023). Primarni cilj računovodstva je torej zagotoviti koristne informacije za odločanje deležnikom, kot so lastniki, vodstvo, upniki, vlagatelji itd. (GBPSSI, brez datuma).

2.1 Vrste računovodstev

V podjetju je prisotna velika količina podatkov in informacij. Nastajajo na podlagi podatkov, ki so ključnega pomena za vodstvene odločitve, zato je treba jasno ločiti, kateri podatki so namenjeni javnosti in kateri morajo ostati znotraj podjetja. Zaradi tega računovodstvo v podjetjih delimo na stroškovno, finančno in poslovodno (Lončar, 2009):

a. Stroškovno računovodstvo se osredotoča na notranje poslovanje podjetja in je analitične narave. Njegova glavna vloga je spremljanje in proučevanje stroškov, povezanih z materiali, s storitvami, z delom in amortizacijo. Hkrati analizira učinke poslovnega procesa – izdelke in storitve – ter ocenjuje poslovni izid za posamezne enote znotraj podjetja. Namenjeno je notranjemu nadzoru in izboljševanju učinkovitosti (Igličar in drugi, 2017).
b. Finančno računovodstvo se ukvarja z beleženjem poslovnih dogodkov in s pripravo računovodskih izkazov, namenjenih zunanjim uporabnikom. Njegov glavni namen je zagotavljanje preglednih in verodostojnih informacij o premoženju, obveznostih, kapitalu, prihodkih in odhodkih podjetja. Te informacije so ključne za zunanje deležnike, kot so investitorji, posojilodajalci, državni organi in drugi, ki na njihovi osnovi sprejemano pomembne poslovne in finančne odločitve. Podatki so predstavljeni v denarnih merskih enotah, njihova pravilnost pa je zakonsko predpisana in nadzorovana. Finančno računovodstvo s tem zagotavlja transparentnost poslovanja ter podlago za obdavčitev in poročanje (Igličar in drugi, 2017).
c. Poslovodno računovodstvo je usmerjeno k potrebam notranjih uporabnikov, predvsem vodstva podjetja. Njegov cilj je priprava informacij, ki jih potrebujejo za odločanje. Rezultat poslovodnega računovodstva so navadno analize in študije točno določenih problemov (Čadež, 2013). Igličar in drugi (2017) nadaljujejo, da temelji na podatkih iz finančnega in stroškovnega računovodstva, ko jih nadgrajuje in prilagaja za specifične potrebe podjetja. Informacije niso omejene le na denarne kazalnike, ampak vključujejo tudi količinske podatke, kot so število zaposlenih, porabljene delovne ure, količina uporabljenega materiala ipd. Čadež (2013) dodaja, da v primerjavi s finančnim

računovodstvom tukaj ni zakonskih zahtev glede oblike in vsebine poročanja, vendar ima kljub temu velik vpliv na kakovost in uspešnost poslovnega odločanja.

2.2 Računovodski izkazi

Računovodsko poročanje omogoča primerljivost med podjetji, saj vsa uporabljajo enotne oblike poročil. Postopek vključuje evidentiranje poslovnih dogodkov, njihovo razvrščanje, knjiženje v glavno knjigo in povzemanje podatkov. Glavne kategorije računovodstva so sredstva, obveznosti, kapital, prihodki in odhodki, ki se razvrstijo v bilanci stanja in izkazu poslovnega izida. Nadaljuje, da vsako podjetje uporablja svoj kontni načrt, ki podrobneje določa posamezne postavke (npr. najemnina, amortizacija, plače). Bilanca stanja prikazuje stanja sredstev, obveznosti in kapitala, izkaz poslovnega izida pa prihodke in odhodke. Za celovit vpogled v poslovanje podjetja morata biti vedno predstavljena oba izkaza skupaj (Layton, 2020).

Robnik (2008) bilanco stanja opredeljuje kot temeljni računovodski izkaz, ki prikazuje premoženjsko in finančno stanje podjetja na določen dan. Sestavljena je iz dveh enakovrednih delov – aktiva prikazuje sredstva podjetja, razvrščena glede na njihovo obliko in ročnost, pasiva pa prikazuje vire financiranja teh sredstev – lastniški kapital in obveznosti (dolgovi). Poudarja, da je temeljno načelo bilance, da mora biti skupna vrednost sredstev enaka skupni vrednosti virov sredstev, kar zagotavlja bilančno ravnotežje. Bilanca se običajno sestavi ob koncu poslovnega leta, lahko pa tudi ob drugih priložnostih (npr. ob združitvah, prenehanju podjetja ali menjavi vodstva).

Schnidt (2025) je izkaz poslovnega izida označil kot temeljni računovodski izkaz, ki izraža dobičkonosnost podjetja. Robnik (2008) nadaljuje, da prikazuje, koliko prihodkov in odhodkov je podjetje ustvarilo v določenem obdobju ter kakšen je bil rezultat poslovanja – dobiček ali izguba. V izkazu so zajeti vsi poslovni dogodki ob njihovem nastanku (ne glede na dejansko plačilo), kar pomeni, da temelji na nastanku poslovnega dogodka in ne na denarnem toku. Poslovni izid predstavlja razliko med prihodki in odhodki ter je pozitiven, če podjetje posluje z dobičkom, in negativen, če ustvari izgubo.

Robnik (2008) navaja, da je izkaz denarnih tokov računovodski izkaz, ki prikazuje, kako so prejemki in izdatki v določenem obdobju vplivali na stanje denarnih sredstev podjetja. Trdi, da prikazuje denarne tokove iz treh glavnih dejavnosti: poslovanja, investiranja (nakupi in prodaje sredstev) in financiranja (npr. najem posojil ali izplačilo dividend). Lahko se sestavi po neposredni ali posredni metodi, odvisno od razpoložljivih podatkov. Namen izkaza je prikazati, kako se denar giblje skozi podjetje in kako to vpliva na njegovo likvidnost.

Izkaz gibanja kapitala Robnik (2008) opredeli kot računovodski izkaz, ki prikazuje spremembe v sestavinah kapitala podjetja v določenem obdobju, kot so osnovni kapital, rezerve, čisti dobiček ali izguba ter morebitni prevrednotovalni presežki. Prikazuje, kako se te postavke spreminjajo zaradi poslovanja, razdelitve dobička, pokrivanja izgub ali drugih

določitev lastnikov. Poseben poudarek ima tudi izračun bilančnega dobička, ki ga družba lahko razporedi delničarjem, v rezerve, za prenos v prihodnje leto ali za druge namene.

2.3 Zakonska podlaga in strokovni okvirji računovodstva v Sloveniji

Finančno računovodstvo mora pri poročanju za zunanje uporabnike temeljiti na zakonskih predpisih, računovodskih standardih in drugih strokovnih priporočilih ter usmeritvah (Igličar in drugi, 2017). V Republiki Sloveniji je računovodstvo urejeno na dva načina. Za zasebna podjetja veljajo splošna pravila računovodenja, ki jih določa 54. člen Zakona o gospodarskih družbah (ZGD-1), Uradni list RS, št. 65/09 – uradno prečiščeno besedilo, 33/11, 91/11, 32/12, 57/12, 44/13 – odl. US, 82/13, 55/15, 15/17, 22/19 – ZPosS, 158/20 – ZIntPK-C, 18/21, 18/23 – ZDU-1O, 75/23 in 102/24. Ta podjetja so dolžna voditi poslovne knjige in pripravljati letna poročila v skladu s Slovenskimi računovodskimi standardi (v nadaljevanju SRS), ki jih sprejema Slovenski inštitut za revizijo s predhodnim soglasjem Ministrstva za finance Republike Slovenije in Ministrstva za gospodarstvo Republike Slovenije.

Za poračun, proračunske uporabnike, pravne osebe javnega prava in pravne osebe zasebnega prava, ki ne vodijo poslovnih knjig po ZGD-1, pa veljajo določila Zakona o računovodstvu (ZR) Uradni list RS, št. 23/99, 30/02 – ZJF-C in 114/06 – ZUE, kot je opredeljeno v 1. členu ZR. Temelj za njihovo računovodsko ureditev predstavljata tudi Zakon o gospodarskih javnih službah (ZGJS) Uradni list RS, št. 32/93, 30/98 – ZZLPPO, 127/06 – ZJZP, 38/10 – ZUKN in 57/11 – ORZGJS40 in Zakon o društvih (ZDru-1) Uradni list RS, št. 32/93, 30/98 – ZZLPPO, 127/06 – ZJZP, 38/10 – ZUKN in 57/11 – ORZGJS40. Pripravo ZR in podzakonskih aktov, sprejetih na njegovi podlagi, vodi Ministrstvo za finance Republike Slovenije. Področje računovodstva dodatno ureja še Zakon o javnih financah (ZJF) Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13, 55/15 – ZFisP, 96/15 – ZIPRS1617, 13/18, 195/20 – odl. US, 18/23 – ZDU-1O, 76/23, 24/25 – ZFisP-1 in 39/25, in sicer v 8. poglavju, pri čemer so pristojnosti računovodske službe natančneje določene v 91. členu, če s posebnim zakonom ni določeno drugače.

2.3.1 Zakon o gospodarskih družbah

ZGD-1 predstavlja temeljni pravni akt za delovanje gospodarskih subjektov v Sloveniji in vsebuje tudi številne določbe, ki so neposredno pomembne za področje računovodstva. Ključna zahteva je, da morajo gospodarske družbe voditi poslovne knjige in sestavljati letna poročila v skladu z zakonom in računovodskimi standardi. Poslovne knjige morajo izkazovati resnično in pošteno sliko stanja podjetja, kar pomeni, da morajo biti podatki verodostojni, primerljivi in razumljivi, kar je tudi bistveno za kakovostno računovodsko poročanje (54. člen ZGD-1).

Letno poročilo, kot ga predpisuje ZGD-1, mora vsebovati najmanj bilanco stanja, izkaz poslovnega izida, priloge s pojasnili, podatke o poslovanju družbe in izjavo poslovodstva o

odgovornosti za pripravo poročila (55. člen ZGD-1). Poleg tega morajo srednje in velike družbe ter nekatere druge (npr. družbe javnega interesa) pripraviti tudi revizijo letnega poročila, kar pomeni, da morajo biti računovodski izkazi pripravljeni skladno z vsemi predpisi in standardi, saj jih bo pregledal pooblaščeni revizor (57. člen ZGD-1).

ZGD-1 določa tudi roke in vsebinske zahteve. Te predstavljajo pomembne okvire za računovodje, ki skrbijo za skladnost finančnega poročanja in pravočasno oddajo zakonsko predpisanih dokumentov. Družbe morajo letno poročilo sestaviti najkasneje v treh mesecih po koncu poslovnega leta, v primeru zavezancev za revizijo pa v štirih mesecih (58. člen ZGD-1). Poleg tega zakon nalaga obveznost predložitve poročila AJPES-u za javno objavo (58. člen ZGD-1).

2.3.2 Slovenski računovodski standardi

Slovenski računovodski standardi 2024 (SRS 2024) Uradni list RS, št. 129/23 predstavljajo temeljna strokovna pravila na področju računovodstva, ki jih pripravlja Slovenski inštitut za revizijo. Njihova vzpostavitev izhaja iz 5. člena Zakona o računovodstvu iz leta 1989, ki je oblikovanje standardov prenesel na strokovno organizacijo. S tem je bilo omogočeno boljše prilagajanje sodobnim trendom v računovodstvu doma in v tujini (SRS, 2024).

S 1. januarjem 2024 so v veljavo stopili prenovljeni SRS 2024, ki so nadomestili različico iz leta 2016. Temeljijo na ZGD-1 in vključujejo določila Direktive 2013/34/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o letnih računovodskih izkazih, konsolidiranih računovodskih izkazih in povezanih poročilih nekaterih vrst podjetij, spremembi Direktive 2006/43/ES Evropskega parlamenta in Sveta ter razveljavitvi direktiv Sveta 78/660/EGS in 83/349/EGS, kar zagotavlja usklajenost z evropsko zakonodajo (SRS, 2024).

SRS-ji dopolnjujejo zakonske določbe z razčlenitvami in navodili za uporabo v praksi. Novi standardi se osredotočajo na finančno računovodenje za zunanje uporabnike, medtem ko notranje obračune in davčne vidike urejajo drugi predpisi. Pravila skrbnega računovodenja (PSR) zdaj dopolnjujejo finančni okvir (SRS, 2024). PSR določajo ravnanje s knjigovodskimi listinami kot podlago za evidentiranje poslovnih dogodkov, vključno z njihovo opredelitvijo, s sestavljanjem, prenašanjem, kontroliranjem, knjiženjem in hrambo (PSR, 2016). Prenovljeni SRS-ji uvajajo enotna računovodska pravila (pripoznavanje, merjenje in vrednotenje) za vse organizacije, z dodatnimi usmeritvami za posebne primere, kot so socialna podjetja (SRS, 2024).

2.3.3 Zakon o računovodstvu

ZR je razdeljen na šestnajst poglavij, ki obravnavajo različna področja računovodskega poslovanja. Med temi so knjigovodske listine in poslovne knjige, razčlenjevanje prihodkov in odhodkov, določanje izida poslovanja ter priprava računovodskih izkazov in letnih

poročil. Prav tako se zakon posveča hrambi knjigovodskih listin, vrednotenju postavk, popisu sredstev in obveznosti, odpisovanju dolgoročnih sredstev, predlaganju in posredovanju letnih poročil ter izvajanju računovodske kontrole (Ministrstvo za finance, 2025).

ZR ureja vodenje poslovnih knjig in pripravo letnih poročil za proračun, proračunske uporabnike, pravne osebe javnega prava in nekatere zasebne subjekte, ki niso zajeti v drugih zakonih, kot so ZGD-1, ZGJS ali ZDru-1. Za pripravo zakona in pripadajočih podzakonskih aktov je pristojno Ministrstvo za finance Republike Slovenije. Namen zakona je zagotoviti enotne in pregledne računovodske prakse, kar krepi finančno transparentnost in odgovornost v javnem sektorju ter določenih zasebnih organizacijah v Sloveniji (1. člen ZR).

Pravne osebe morajo voditi poslovne knjige in sestavljati letna poročila v skladu z računovodskimi standardi, ki jih izdaja Slovenski inštitut za revizijo (2. člen ZR). Računovodski izkazi, ki jih sestavljajo pravne osebe, vključujejo bilanco stanja, izkaz prihodkov in odhodkov, letno poročilo ter tudi pojasnila in poslovno poročilo (20.–21. člen ZR). Ob koncu leta se obvezno opravita popis sredstev in obveznosti ter uskladitev stanj s knjigovodskim stanjem (36. člen ZR). Letna poročila se morajo predložiti najkasneje do konca februarja naslednjega leta in jih mora podpisati pooblaščena oseba pravne osebe (26.–27. člen ZR).

2.3.4 Mednarodni standardi računovodskega poročanja

Mednarodni standardi računovodskega poročanja (v nadaljevanju MSRP) so namenjeni poenotenju računovodskih praks pri zunanjem finančnem poročanju na mednarodni ravni. Njihov cilj je zagotoviti pregledno, zanesljivo in primerljivo poročanje, kar krepi zaupanje v finančne informacije, olajšuje dostop do mednarodnih kapitalskih trgov in podpira učinkovitejše upravljanje mednarodnih podjetij (Igličar in drugi, 2017). Pravni akt EU, s katerim so standarde MSRP vključili v pravni red EU, je Uredba Komisije (EU) 2023/1803 z dne 13. avgusta 2023 o sprejetju nekaterih mednarodnih računovodskih standardov v skladu z Uredbo (ES) št. 1606/2002 Evropskega parlamenta in Sveta, UL L 237.

K uporabi MSRP so zavezane družbe, ki sestavljajo konsolidirano letno poročilo, banke, zavarovalnice in druge družbe, če tako določi njihova skupščina. Tako določa 54. člen ZGD-1. MSRP so standardi, sprejeti na ravni EU, medtem ko SRS izhajajo iz nacionalne zakonodaje in morajo biti skladni z ZGD-1, direktivo 2013/34/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o letnih računovodskih izkazih, konsolidiranih računovodskih izkazih in povezanih poročilih nekaterih vrst podjetij, spremembi Direktiva 2006/43/ES Evropskega parlamenta in Sveta z dne 17. maja 2006 o obveznih revizijah za letne in konsolidirane računovodske izkaze, spremembi direktiv Sveta 78/660/EGS in 83/349/EGS ter razveljavitvi Direktive Sveta 84/253/EGS, Uradni list EU 182, in ne smejo biti v nasprotju z MSRP. Postopoma stare MRS-standarde nadomeščajo z novimi MSRP.

Poznavanje SRS, ki temeljijo na direktivah EU, domačim računovodjam olajša razumevanje vsebine MSRP (Kamenšek, 2022).

2.4 Računovodski servisi

Računovodski servis je združba, ki lahko vključuje enega ali več računovodskih strokovnjakov, ki vsak zase spoštujejo temeljna načela svoje stroke (ZRS, 2025b). V širšem gospodarskem prostoru imajo računovodski servisi pomembno vlogo, še posebej na področju malega gospodarstva. Že v zgodnjih fazah razvoja so prepoznali potrebo po povezovanju, zato so si leta 1996 začeli prizadevati za ustanovitev lastnega združenja znotraj Gospodarske zbornice Slovenije. Tako je 3. decembra 1996 nastala Sekcija podjetij računovodskih, knjigovodskih, revizijskih in davčno svetovalnih storitev (v nadaljevanju SRKRD). Ta se je leta 1998 preoblikovala v samostojno Združenje računovodskih servisov, ki je 1. januarja 2009 dobilo novo ime – Zbornica računovodskih servisov (v nadaljevanju ZRS) (ZRS, 2025b). Leta 2013 je ZRS sprejela kodeks članov, ki temelji na mednarodnih etičnih načelih in dopolnjuje zakonodajo. Kodeks določa odgovornost do okolja, naročnikov in zaposlenih, pri čemer poudarja strokovnost, nepristranskost, varovanje zaupnosti ter spoštljiv odnos do konkurence in lokalne skupnosti. Od zaposlenih zahteva celovitost, objektivnost, profesionalnost in zaupnost, od vodij pa zagotavljanje ustreznih pogojev dela in stalnega izobraževanja. Člani ZRS so zavezani k spoštovanju kodeksa, pri čemer njegovo upoštevanje prispeva k ugledu in razvoju računovodske stroke (ZRS, 2025b).

Računovodski servisi niso namenjeni zgolj pripravi davčnih obračunov, ampak podjetjem ponujajo širok spekter storitev, ki so ključne za učinkovito finančno poslovanje (Miller, 2022). Izvajajo širok nabor računovodskih in knjigovodskih storitev, ki vključujejo vodenje temeljnih poslovnih knjig (kontiranje in knjiženje dokumentov), obračune obresti, vodenje plačilnega prometa, materialno knjigovodstvo ter spremljanje saldakontov kupcev in dobaviteljev. Poleg tega skrbijo za obračune DDV-ja, vodenje davčnih evidenc, pripravo poročil, vodenje blagajne in registra osnovnih sredstev z obračuni amortizacije, s pripravo amortizacijskih načrtov in z različnimi administrativnimi opravili, kot sta npr. fakturiranje ter priprava predlogov za kompenzacijo, cesijo in asignacijo (Informa studio d. o. o., 2025).

Računovodski servisi nudijo tudi obračune osebnih prejemkov, pri katerih pripravljajo podatke, izračunavajo plače in druge prejemke, vodijo mesečno poročanje in pripravljajo plačilne naloge. Poleg obračuna plač in regresa skrbijo tudi za obračune socialnih prispevkov, izplačila dodatnih dohodkov, kot so jubilejne nagrade ali avtorski honorarji, ter poročajo na različne uradne institucije. Nudijo tudi dodatne kadrovske storitve, kot so vodenje osebnih evidenc, prijave in odjave zavarovanj ter svetovanje o zakonodaji (Informa studio d. o. o., 2025).

V okviru svojih storitev računovodski servisi nudijo tudi strokovno davčno, finančno in poslovno svetovanje, s katerim podjetjem pomagajo optimizirati poslovanje in izboljšati obvladovanje ter načrtovanje finančnih procesov. Na področju davkov svetujejo pri različnih

vrstah davkov, zniževanju davčnega tveganja, popravljanju napak, pri pripravi transfernih cen in zastopanju pred davčnimi organi. Na področju finančnega svetovanja pomagajo pri iskanju financiranja, ocenjevanju donosnosti investicij, sanaciji prezadolženosti, analizah poslovnih kazalnikov ter spremljanju zakonodaje in pripravi potrebne dokumentacije za revizijo in pogodbena razmerja (Informa studio d. o. o., 2025).

Sodobni računovodski servisi poleg strokovnega znanja uporabljajo tudi napredno tehnologijo, ki omogoča sprotno usklajevanje računov, avtomatiziranje postopke, ažurno poročanje in vpogled v finančno stanje podjetja v realnem času. Tako ne zagotavljajo le skladnosti z zakonodajo, temveč postajajo tudi pomembni partnerji pri rasti, optimizaciji in dolgoročni uspešnosti podjetja (Miller, 2022).

2.4.1 Računovodstvo kot poklic

Računovodstvo danes ni več omejeno le na pripravo številk in poročil, temveč ima pomembno vlogo pri poslovnem odločanju. Sodobni računovodja je dejavno vključen v razlago računovodskih informacij in sodeluje pri oblikovanju poslovne strategije podjetja. Poudarjajo, da zaradi avtomatizacije in tehnološkega razvoja računovodje več sodelujejo z vodstvom podjetja ter delujejo na področjih, kot so finance, proizvodnja in prodaja. Z razvojem vloge računovodij se je povečal tudi njihov ugled. Menijo, da njihovo delo postaja zanimivejše, bolj vizionarsko in proaktivno. Poleg strokovnega znanja je danes za računovodje zelo pomembna sposobnost komunikacije in dela z ljudmi, saj pogosto sodelujejo z vodilnimi kadri, s strankami, z dobavitelji, bančniki, davčnimi organi in s svetovalci. Te veščine so ključne tudi za prevzemanje vodilnih položajev (Igličar in drugi, 2017).

Igličar in drugi (2017) opozarjajo, da se sodobni računovodje srečujejo tudi z izzivi etične narave. Včasih so pod pritiskom poslovodstva, da prilagodijo računovodske metode z namenom prikaza boljših poslovnih rezultatov. Nadaljujejo, da morajo v takšnih primerih ohraniti svojo strokovnost, zakonitost in osebno integriteto. Pri tem jim pomaga Kodeks etike za računovodske strokovnjake, ki določa pet osnovnih načel:

a. neoporečnosti – biti pošten in iskren v vseh poklicnih odnosih,
b. nepristranskost – izogibati se pristranskosti in neprimernemu vplivu,
c. zagotavljati strokovno usposobljenost in skrbnost,
d. zaupnost – varovati zaupne informacije in jih ne zlorabiti,
e. poklicno primerno vedenje – spoštovati predpise in ugled poklica.

Igličar in drugi (2027) poudarjajo, da imajo računovodski strokovnjaki številne možnosti zaposlitve. Delajo lahko kot računovodje v podjetjih ali samostojno, postanejo lahko revizorji, davčni ali poslovni svetovalci ter opravljajo druge strokovne naloge v finančnih institucijah in oddelkih. Jackson in drugi (2023) menijo, da mladi računovodje pri svojih poklicnih odločitvah pogosto dajejo največjo vrednost stabilnosti zaposlitve, usklajenosti

poklicnega in zasebnega življenja ter priložnostim za karierni napredek. Vendar pa izpostavljajo, da se njihova pričakovanja ob vstopu v poklic pogosto ne ujemajo s stvarnimi izkušnjami na delovnem mestu, kar lahko negativno vpliva na njihovo zadovoljstvo in zadrževanje v poklicu na dolgi rok. Zato je ključno, da imajo mladi računovodje na voljo kakovostno izobraževanje in mentorstvo, ki jim pomaga pri učinkovitem soočanju s poklicnimi izzivi ter doseganju osebnih in strokovnih ciljev. Burke in Polimeni (2023) dodajata, da so poleg tega mladi vse manj zainteresirani za računovodski poklic zaradi nizkih začetnih plač, dolgega delovnega časa in slabšega ravnotežja med poklicnim in zasebnim življenjem.

Igličar in drugi (2017) zaključujejo, da se v Sloveniji računovodje, finančniki in revizorji povezujejo v Zvezo računovodij, finančnikov in revizorjev Slovenije (v nadaljevanju ZRFR). Ta organizacija podpira razvoj stroke z izobraževanji, izmenjavo znanja, izdajo strokovne literature ter s sodelovanjem pri pripravi zakonodaje in standardov.

3 ZAKONSKA PODLAGA VARSTVA OSEBNIH PODATKOV V SLOVENIJI

Varstvo osebnih podatkov je v Sloveniji pravno urejeno predvsem s Splošno uredbo o varstvu podatkov, ki se neposredno uporablja v vseh državah članicah Evropske unije, ter z nacionalnim ZVOP-2, ki dopolnjuje uredbo z dodatnimi pravili in obveznostmi. Osrednji namen zakonodaje je zagotoviti, da se osebni podatki obdelujejo varno, zakonito in pregledno, pri čemer je varnost podatkov eden od temeljnih stebrov celotnega sistema varstva. Pravna podlaga tako zahteva od upravljavcev in obdelovalcev, da sprejmejo ustrezne tehnične in organizacijske ukrepe za zaščito pred nepooblaščenim dostopom, razkritjem, izgubo ali uničenjem podatkov, ob upoštevanju narave obdelave in ocenjenih tveganj. ZVOP-2 dodatno ureja posebne vidike, kot so vodenje dnevnikov obdelave, obdelava posebej občutljivih podatkov in posebne zahteve za državne registre ter informacijske sisteme, kar skupaj predstavlja celovit normativni okvir za zagotavljanje varnosti in zakonitosti obdelave osebnih podatkov v slovenskem prostoru (IPRS, 2025c).

3.1 Splošna uredba o varstvu osebnih podatkov

Evropska unija je 4. maja 2016 sprejela ključna dokumenta na področju varstva osebnih podatkov – Splošno uredbo (GDPR) in Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, ter o prostem pretoku takih podatkov in o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ. GDPR, ki se uporablja od 25. maja 2018, je nadomestila Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter uvedla enotne standarde varstva osebnih podatkov v EU. Direktiva o

kazenskem pregonu je bila v slovensko zakonodajo prenesena z Zakonom o varstvu osebnih podatkov na področju kaznivih dejanj (ZVOPOKD) Uradni list RS, št. 177/20, leta 2023 pa je sledil še ZVOP-2 (IPRS, 2025a). Reforma, predlagana že leta 2012, je odziv na izzive, ki jih prinašajo digitalne tehnologije, kot so družbena omrežja, računalništvo v oblaku in mobilne naprave ter naraščajoč obseg obdelave podatkov. Glavni cilji so zaščita temeljnih pravic posameznikov, razvoj digitalnega gospodarstva ter učinkovitejši boj proti kriminalu in terorizmu (IPRS, 2025a).

GDPR v 4. členu določa, da so osebni podatki kakršne koli informacije, ki se nanašajo na določeno ali določljivo posamezno osebo. Primeri takšnih podatkov so na primer ime, priimek, telefonske številke strank, deležnikov, zaposlenih ali ponudnikov; identifikacijske številke, kot so številke strank, številke zaposlenih ali reference rezervacij; e-poštni naslovi, podatki o lokaciji, zgodovina brskanja, zgodovina nakupov in računi; ter fotografije, videoposnetki in zvočni posnetki z osebami. S temi podatki je mogoče posameznika prepoznati neposredno (na primer z imenom ali s priimkom) ali posredno (na primer z referenčno številko ali s številko stranke). Poleg tega se kot osebni podatki štejejo tudi vse informacije, povezane z neposredno ali s posredno prepoznavno osebo, kot so njene preference ali navade (4. člen GDPR).

3.1.1 Pravni okvir obdelave osebnih podatkov po splošni uredbi

V 5. členu GDPR je določeno, da obdelava osebnih podatkov temelji na več ključnih načelih, ki zagotavljajo zakonito in pravično ravnanje z njimi. Podatki morajo biti obdelani na zakonit, pošten in pregleden način v zvezi s posameznikom, na katerega se nanašajo. Zbirajo in obdelujejo se lahko le za vnaprej določene, izrecne in zakonite namene, pri čemer je kasnejša obdelava za arhiviranje, raziskovanje ali statistične namene dovoljena le, če je skladna s prvotnimi cilji. Pri tem velja načelo najmanjšega obsega podatkov, kar pomeni, da se zbirajo le tisti podatki, ki so nujno potrebni za določen namen. Pomembno je tudi načelo točnosti, ki zahteva, da so podatki pravilni in redno posodobljeni, netočni podatki pa morajo biti brez odlašanja popravljeni ali izbrisani. Osebni podatki morajo biti shranjeni le toliko časa, kolikor je potrebno za dosego namena obdelave, daljše shranjevanje pa je dopustno le za posebne namene ob ustreznih varnostnih ukrepih. Zagotovljeni morata biti celovitost in zaupnost, kar pomeni, da morajo biti podatki varovani pred nedovoljeno obdelavo, izgubo, uničenjem ali poškodbo z uporabo ustreznih tehničnih in organizacijskih ukrepov. Načelo odgovornosti določa, da je upravljavec osebnih podatkov odgovoren za zagotavljanje skladnosti s temi načeli in mora biti sposoben skladnost tudi dokazati. Ta načela so osnova za visoke standarde varstva osebnih podatkov in zaščito pravic posameznikov (5. člen GDPR).

Po 7. členu GDPR mora biti privolitev posameznika za obdelavo osebnih podatkov dana prostovoljno, jasno in razumljivo, upravljavec pa mora biti sposoben dokazati, da je bila resnično podana. Če je privolitev del pisne izjave, ki vključuje tudi druge vsebine, mora biti

jasno ločena, napisana v preprostem jeziku in preprosta za razumevanje. Deli, ki ne izpolnjujejo teh zahtev, niso pravno zavezujoči. Posameznik lahko svojo privolitev kadar koli prekliče brez vpliva na zakonitost obdelave pred preklicem. O tej pravici in načinu preklica mora biti jasno obveščen, postopek pa mora biti enako preprost kot podaja privolitve. Privolitev prav tako ne sme biti pogoj za sklenitev pogodbe, razen če je obdelava osebnih podatkov nujna za njeno izvedbo. S tem se zagotavlja, da je privolitev resnično svobodna in brez prisile (7. člen GDPR).

GDPR v 6. členu določa, da lahko upravljavci osebne podatke obdelujejo le, če za to obstaja ustrezna pravna podlaga. To je lahko privolitev posameznika, ki mora biti prostovoljna, informirana, specifična in nedvoumna. Gre lahko za obdelavo, ki je potrebna za izpolnitev pogodbene obveznosti med posameznikom in organizacijo ali za izpolnjevanje zakonskih obveznosti, ki veljajo za upravljavca. Obdelava je mogoča tudi pri izvajanju javnih nalog v javnem interesu ali v primerih, ko je treba varovati življenjske interese posameznika, ki sam ni bil sposoben dati privolitve. Poleg tega je obdelava osebnih podatkov dovoljena zaradi zakonitih interesov upravljavca ali tretje osebe, razen kadar nad temi interesi prevladajo interesi temeljne pravice ali svoboščine posameznika. Za obdelavo občutljivih osebnih podatkov GDPR določa še dodatne posebne pogoje (6. člen GDPR).

3.1.2 Pravice posameznika, na katerega se nanašajo osebni podatki

Eden izmed pomembnih ciljev Splošne uredbe o varstvu osebnih podatkov je bil poenotiti in okrepiti pravice posameznikov v zvezi z obdelavo njihovih osebnih podatkov. V okviru te ureditve so organizacije dolžne posameznike jasno in pravočasno obvestiti o njihovih pravicah ter jim omogočiti, da jih učinkovito uveljavljajo (Jamšek, 2018).

Upravljavec osebnih podatkov mora posameznikom zagotoviti jasne, pregledne in razumljive informacije o obdelavi njihovih podatkov ter jim omogočiti uresničevanje pravic iz 15.–22. člena GDPR. Informacije se morajo posredovati pisno ali elektronsko brez nepotrebnega odlašanja, najpozneje v enem mesecu po prejemu zahteve. Rok se lahko v zapletenih primerih podaljša za dodatna dva meseca. Storitve so brezplačne, razen kadar so zahteve očitno neutemeljene ali pretirane. Ob dvomu o identiteti lahko upravljavec zahteva dodatna pojasnila. Za večjo preglednost se lahko uporabljajo tudi standardizirane ikone, kot jih določi Evropska komisija (12. člen GDPR). Če upravljavec podatke pridobi neposredno od posameznika, ga mora obvestiti o svoji identiteti, namenih in pravni podlagi obdelave, uporabniki podatkov, morebitnih prenosih v tretje države, obdobju hrambe ter pravicah, kot so dostop, popravek, izbris, ugovor in prenosljivost. Posameznik mora biti seznanjen tudi s pravico do pritožbe, posledicami nepredložitve podatkov, z obstojem avtomatiziranega odločanja in morebitnimi spremembami namenov obdelave. Te informacije ni treba ponovno posredovati, če jih posameznik že ima (13. člen GDPR). Kadar osebni podatki niso pridobljeni neposredno od posameznika, mora upravljavec zagotoviti enakovreden nabor informacij: svojo identiteto, namen in pravno podlago obdelave, vir podatkov, obdobje

hrambe, pravice posameznika, morebitne prenose in avtomatizirano odločanje. Podatke mora posredovati najpozneje v enem mesecu, ob prvem stiku ali ob prvem razkritju osebi, razen kadar bi bilo to nemogoče, nesorazmerno, obremenjujoče ali zakonsko prepovedano (14. člen GDPR).

V 15. členu GDPR določa, da ima posameznik pravico od upravljavca pridobiti potrditev, ali se njegovi osebni podatki obdelujejo. Če je tako, mu mora biti omogočen dostop do podatkov in informacij o namenu obdelave, vrstah podatkov, uporabnikih, ki jim bodo razkrili, vključno z morebitnimi prenosi v tretje države ali mednarodne organizacije. Upravljavec mora posredovati tudi podatke o predvidenem obdobju hrambe ali merilih za njegovo odločitev, pravicah posameznika (popravek, izbris, omejitev obdelave, ugovor), možnosti pritožbe pri nadzornem organu, izvoru podatkov (če niso bili pridobljeni neposredno) ter morebitnem avtomatiziranem odločanju, vključno s profiliranjem in z njegovimi posledicami. Če pride do prenosa podatkov v tretje države ali mednarodne organizacije, mora biti posameznik obveščen o ustreznih zaščitnih ukrepih, ki zagotavljajo varen prenos. Posameznik ima pravico prejeti kopijo osebnih podatkov, ki se obdelujejo. Dodatne kopije lahko upravljavec zaračuna, vendar po razumni ceni. Če je zahteva podana elektronsko, se podatki praviloma posredujejo v elektronski obliki, razen če posameznik zahteva drugače. Ta pravica ne sme posegati v pravice in svoboščine drugih oseb (15. člen GDPR).

Po 16. členu GDPR ima posameznik pravico zahtevati, da upravljavec brez nepotrebnega odlašanja popravi netočne osebne podatke, ki se nanašajo nanj. Poleg tega lahko posameznik zahteva dopolnitev nepopolnih osebnih podatkov, če so namenjeni za obdelavo, pri čemer lahko za dopolnitev predloži tudi dopolnilno izjavo (16. člen GDPR).

Na podlagi 17. člena GDPR lahko posameznik od upravljavca zahteva izbris svojih osebnih podatkov brez nepotrebnega odlašanja, če podatki niso več potrebni za namen, za katerega so bili zbrani, če prekliče privolitev, uspešno ugovarja obdelavi, če so bili podatki obdelani nezakonito ali če izbris zahteva zakon. Enako velja za podatke, zbrane pri ponudbi storitev informacijske družbe mladoletnikom. Če so bili podatki javno objavljeni, mora upravljavec sprejeti razumne ukrepe, da o zahtevi za izbris obvesti druge upravljavce, ki podatke obdelujejo. Pravica do izbrisa ni absolutna. Ne velja, kadar je obdelava nujna zaradi svobode izražanja, izpolnjevanja zakonskih obveznosti, javnega interesa, varovanja javnega zdravja, znanstveno raziskovalnih ali statističnih namenov ali za uveljavljanje pravnih zahtevkov. Tako imenovana pravica do pozabe posameznikom omogoča večji nadzor nad lastnimi podatki, a mora biti vedno v ravnotežju z drugimi legitimnimi interesi in pravicami (17. člen GDPR).

Pravica iz 18. člena GDPR določa, da lahko posameznik zahteva omejitev obdelave osebnih podatkov v določenih primerih. To velja, kadar oporeka točnosti podatkov in je potrebna njihova preverba, kadar je obdelava nezakonita, a ne želi izbrisa, ali če podatkov upravljavec sicer ne potrebuje več, posameznik pa jih potrebuje za uveljavljanje pravnih zahtevkov.

Omejitev je mogoča tudi ob vloženem ugovoru, dokler se ne razjasni, kateri interesi prevladujejo. Ob omejitvi je dovoljena le hramba podatkov, nadaljnja obdelava pa le s privolitvijo posameznika, za pravne postopke, zaščito pravic drugih ali v javnem interesu. Preden omejitev preneha veljati, mora upravljavec posameznika o tem obvestiti (18. člen GDPR).

V skladu z 20. členom ima posameznik pravico prejeti svoje osebne podatke v strukturirani, splošno uporabljani in strojno berljivi obliki ter jih brez ovir prenesti k drugemu upravljavcu. To velja, kadar se podatki obdelujejo na podlagi privolitve ali pogodbe z avtomatiziranimi sredstvi. Če je tehnično izvedljivo, lahko posameznik zahteva tudi neposreden prenos med upravljavci. Pravica ne velja za obdelave, ki potekajo v okviru javnega interesa ali izvajanja javne oblasti. Prenosljivost ne sme posegati v pravice drugih oseb in ne vpliva na uveljavljanje pravic do izbrisa (20. člen GDPR).

V 21. členu GDPR določa, da lahko posameznik kadar koli ugovarja obdelavi svojih osebnih podatkov, če ta temelji na zakonitem interesu organizacije ali javnem interesu. V takem primeru mora upravljavec prenehati z obdelavo, razen če dokaže, da ima nujne in prevladujoče razloge za nadaljevanje. Pri obdelavi podatkov za neposredno trženje je pravica do ugovora absolutna – ob vložitvi ugovora mora upravljavec takoj prenehati z obdelavo, tudi pri profiliranju za trženjske namene. Posameznika je treba o tej pravici jasno in ločeno obvestiti že ob prvem stiku. Ugovor je mogoč tudi pri obdelavi za znanstvene, zgodovinske ali statistične namene, če ta ni nujna za naloge v javnem interesu (21. člen GDPR).

Na podlagi 22. člena GDPR ima posameznik pravico, da ni predmet izključno avtomatiziranega odločanja, vključno z oblikovanjem profilov, če bi to imelo pravne učinke ali nanj pomembno vplivalo. Ta pravica ne velja, kadar je odločanje nujno za pogodbo, dovoljeno z zakonodajo, ali temelji na izrecni privolitvi. V takšnih primerih mora upravljavec zagotoviti ustrezne zaščitne ukrepe – omogočiti človeško posredovanje, možnost izražanja mnenja in izpodbijanja odločitve. Odločanje ne sme temeljiti na občutljivih podatkih, razen če zakon to izrecno dopušča ob ustrezni zaščiti pravic posameznika (22. člen GDPR).

3.1.3 Neodvisni nadzorni organ in pooblaščena oseba za varstvo podatkov

Vsaka država članica mora imeti enega ali več neodvisnih nadzornih organov za nadzor nad izvajanjem GDPR, varstvom pravic posameznikov in zagotavljanjem prostega pretoka podatkov znotraj EU. Ti organi med seboj in s Komisijo sodelujejo za usklajeno izvajanje uredbe GDPR (51. člen GDPR). V Sloveniji nadzorni organ predstavlja Informacijski pooblaščenec (5. člen ZVOP-2). Nadzorni organ deluje popolnoma neodvisno. Njegovi člani ne smejo biti pod zunanjim vplivom, države pa morajo zagotoviti ustrezna sredstva, kadrovsko avtonomijo in neodvisen proračun (52. člen GDPR). Organ je pristojen za svojo državo, razen v primerih čezmejne obdelave ali kadar podatke obdelujejo sodišča v okviru sodne funkcije (55. člen GDPR). V čezmejnih primerih je odgovoren vodilni nadzorni organ

– tisti, kjer ima upravljavec ali obdelovalec glavni sedež. Če težava zadeva le eno državo, jo obravnava lokalni nadzorni organ. V primeru širših vplivov morajo lokalni organi obvestiti vodilnega, ki lahko prevzame zadevo in usklajuje postopek z drugimi organi. Če ne, postopek vodi lokali organ sam (56. člen GDPR).

GDPR v 37. členu določa, da morata upravljavec ali obdelovalec imenovati pooblaščeno osebo za varstvo osebnih podatkov (v nadaljevanju DPO), kadar gre za javni organ (razen sodišč), obsežno in sistematično spremljanje posameznikov ali za obsežno obdelavo posebnih vrst podatkov (npr. občutljivih ali kazenskih podatkov). Skupine podjetij ali javni organi lahko imenujejo eno skupno DPO, če je to glede na strukturo smiselno (37. člen GDPR). DPO mora imeti ustrezno strokovno znanje in biti dostopen vsem enotam, Lahko je zaposleni ali zunanji izvajalec. Njeni kontaktni podatki morajo biti javno objavljeni in sporočeni nadzornemu organu (38. člen GDPR). DPO sodeluje pri vseh zadevah varstva osebnih podatkov, ima dostop do informacij in poroča neposredno vodstvu. Deluje neodvisno, brez navodil, ne sme biti kaznovana za svoje delo in mora varovati zaupnost (38. člen GDPR). Njene naloge vključujejo svetovanje in ozaveščanje, spremljanje skladnosti, izvajanje usposabljanj, podporo pri oceni učinkov na varstvo osebnih podatkov, sodelovanje z nadzornim organom in delovanje kot kontaktna točka. Pri delu upošteva naravo in tveganje obdelave (39. člen GDPR).

3.1.4 Ključni dokumenti

Za zagotavljanje skladnosti z GDPR morajo organizacije voditi in vzdrževati določene ključne dokumente. Mednje sodijo evidenca dejavnosti obdelave, informacije, ki jih mora posameznik prejeti ob pridobitvi osebnih podatkov, pogodbe z obdelovalci in ocene učinkov na varstvo osebnih podatkov. Ti dokumenti odražajo načelo odgovornosti in omogočajo preglednost ter pravno varnost pri obdelavi osebnih podatkov (Jamšek, 2018).

a. Evidenca obdelave

V 30. členu GDPR določa, da morajo upravljavci in obdelovalci osebnih podatkov voditi evidenco dejavnosti obdelave. Vključevati mora podatke o upravljavcu, obdelovalcu, njihovih predstavnikih, pooblaščeni osebi za varstvo podatkov, namenih obdelave, kategorijah posameznikov in podatkov, uporabnikih, prenosih v tretje države ter, kjer je mogoče, rokih hrambe in varnostnih ukrepih. Evidenca mora biti pisna (lahko tudi elektronska) in dostopna nadzornemu organu na zahtevo. Izjema velja za organizacije z manj kot 250 zaposlenimi, razen če njihova obdelava ni občasna, vključuje občutljive podatke ali pomeni tveganje za pravice posameznikov. V teh primerih morajo evidenco voditi tudi manjša podjetja (30. člen GDPR).

b. Informacije ob pridobitvi osebnih podatkov od posameznika

Po 13. členu GDPR mora upravljavec, kadar osebne podatke pridobi neposredno od posameznika, temu zagotoviti ključne informacije: identiteto in kontaktne podatke (vključno s pooblaščeno osebo za varstvo osebnih podatkov, če obstaja), namen in pravno podlago obdelave, upravičene interese (če so podlaga za obdelavo), uporabnike podatkov in morebitne prenose v tretje države z navedbo zaščitnih ukrepov. Prav tako mora posameznika obvestiti o trajanju hrambe, njegovih pravicah (dostop, popravek, izbris, omejitev, prenos, ugovor), možnost preklica privolitve in pritožb pri nadzornem organu. Navedeno mora biti tudi, ali je posredovanje podatkov obvezno in kakšne so posledice zavrnitve ter ali poteka avtomatizirano odločanje ali profiliranje. Če želi upravljavec podatke uporabiti za drug namen, mora posameznika o tem predhodno obvestiti, razen če te informacije že ima (13. člen GDPR).

c. Pogodba z obdelovalcem

GDPR v 28. členu določa, da kadar obdelovalec obdeluje osebne podatke v imenu upravljavca, mora zagotoviti ustrezno varnost in spoštovanje pravic posameznikov. Druge obdelovalce lahko vključi le s pisnim soglasjem upravljavca, ki mora biti obveščen o vseh spremembah. Razmerje med upravljavcem in obdelovalcem ureja pisna pogodba, ki določa naravo in obseg obdelave, vrste podatkov, kategorije posameznikov in obveznosti obeh strani. Obdelovalec mora ravnati po navodilih upravljavca, varovati zaupnost, izvajati tehnične in organizacijske ukrepe, pomagati pri izpolnjevanju zakonskih obveznosti in po zaključku obdelave podatke izbrisati ali vrniti. Omogočiti mora tudi revizije. Če meni, da navodila kršijo zakonodajo, mora o tem obvestiti upravljavca. Dodatni obdelovalci morajo spoštovati enake obveznosti kot glavni obdelovalec, ki ostaja odgovoren. Pogodba lahko temelji na standardnih določilih Komisije ali nadzornega organa. Če obdelovalec sam odloča o namenu in sredstvih obdelave, postane upravljavec (28. člen GDPR).

d. Ocena učinka v zvezi z varstvom podatkov

Ocena učinka in varstvo podatkov sta obvezna, kadar obdelava – zlasti z novimi tehnologijami – lahko pomeni visoko tveganje za pravice posameznikov. Opravi se pred začetkom obdelave in lahko zajema več podobnih dejavnosti. Pri tem je treba vključiti pooblaščeno osebo za varstvo osebnih podatkov, če obstaja. Obvezna je pri sistematičnem profiliranju, obsežni obdelavi občutljivih podatkov ali kazenskih evidenc ter ob spremljanju javnih površin. Nadzorni organ določa primere, kjer je ocena obvezna ali ni potrebna. Ocena vključuje opis obdelave in namenov, presojo nujnosti in sorazmernosti, oceno tveganj in ukrepe za njihovo zmanjšanje. Upošteva se skladnost s kodeksi ravnanja. Po potrebi se pridobi mnenje posameznikov, ob upoštevanju poslovnih ali varnostnih interesov. Če zakon določa oceno učinkov, dodatna ocena ni potrebna, razen če to določi država. Upravljavec mora redno preverjati skladnost z oceno, zlasti ob spremembah tveganj (35. člen GDPR). Če ocena pokaže, da kljub ukrepom obstaja visoko tveganje, se mora upravljavec pred začetkom obdelave posvetovati z nadzornim organom. Ta lahko v osmih tednih izda mnenje ali zahteva ukrepe, pri čemer se rok lahko podaljša za šest tednov. Za posvetovanje mora upravljavec

predložiti podatke o načrtovani obdelavi, ocenjene ukrepe in kontakt pooblaščene osebe. Tudi države članice se morajo ob pripravi zakonodaje o obdelavi osebnih podatkov posvetovati z nadzornim organom, zlasti na področjih javnega interesa (36. člen GDPR).

3.2 Zakon o varstvu osebnih podatkov

Področje varstva osebnih podatkov je v Sloveniji dolgo urejal ZVOP-1. Leta 2018 ga je dopolnila Splošna uredba o varstvu osebnih podatkov, ki velja na področju celotne EU. Na začetku leta 2023 je v veljavo stopil ZVOP-2, pri čemer je ZVOP-1 prenehal veljati. ZVOP-2 v Republiki Sloveniji ureja uresničevanje pravice do varstva osebnih podatkov ter določa pogoje za njihovo zakonito in varno obdelavo. Dopolnjuje uredbo GDPR in podrobneje ureja tista področja, ki jih uredba izrecno prepušča državam članicam. Hkrati zagotavlja skladnost slovenske zakonodaje z zahtevami evropskega pravnega reda. Zaradi vzajemnega dopolnjevanja je pri uporabi zakonodaje pomembno celovito upoštevanje tako določb ZVOP-2 kot tudi uredbe GDPR (1. člen ZVOP-2).

ZVOP-2 se uporablja pri avtomatizirani in ročni obdelavi podatkov, kadar so ti del zbirke ali namenjeni vključitvi vanj, ne pa pri obdelavi za osebne ali družinske namene ter pri kazenskih postopkih, ki jih ureja poseben zakon (3. člen ZVOP-2). Zakon izrecno prepoveduje obdelavo osebnih podatkov, ki bi lahko povzročila diskriminacijo posameznika na podlagi osebnih okoliščin (2. člen ZVOP-2). V 4. členu ZVOP-2 določa, da se določbe zakona uporabljajo za vse obdelave osebnih podatkov, ki potekajo v okviru dejavnosti upravljavcev in obdelovalcev, registriranih v Sloveniji. Njegove določbe se uporabljajo tudi v primerih, ko se obdelava izvaja zunaj slovenskega ozemlja, če upravljavec ali obdelovalec deluje v okviru slovenske zakonodaje. Poleg tega se zakon uporablja tudi za ponudnike iz tretjih držav, kadar ponujajo svoje storitve ali izdelke posameznikom v Sloveniji ali spremljajo njihovo vedenje, ne glede na to, ali so storitve brezplačne ali plačljive (4. člen ZVOP-2).

ZVOP-2 v Sloveniji podrobneje ureja obdelavo občutljivih podatkov (zdravstvenih, biometrijskih, genskih), videonadzor, sledljivost obdelave, pooblaščene osebe za varstvo podatkov, postopke izrekanja sankcij ter pravna sredstva in obveznosti v primeru kršitev. Zakon dopolnjuje GDPR, vendar je ne spreminja, saj se uredba uporablja neposredno. Pred uveljavitvijo ZVOP-2 informacijski pooblaščenec ni imel pristojnosti izrekanja glob iz naslova GDPR, ker lokalna zakonodaja ni bila prilagojena. Slovenija je zakon sprejela z zamudo, kot zadnja članica EU (Kovačevič, 2023).

Med pomembnejšimi določbami ZVOP-2 so določitev starosti za privolitev otrok za uporabo storitev informacijske družbe pri 15 letih (8. člen ZVOP-2), omejitev varstva osebnih podatkov umrlih na 20 let po smrti, pri čemer se morajo upoštevati morebitni specialni predpisi, ki lahko določajo drugače (9. člen ZVOP-2). Zakon odpravlja obveznosti poročanja zbirk osebnih podatkov Informacijskemu pooblaščencu in jo nadomešča z vodenjem evidence dejavnosti obdelav. Posebej ureja tudi evidentiranje vstopov in izstopov iz

službenih prostorov ter določa, kateri podatki se smejo zbirati (Kovačevič, 2023). Pomembna novost je tudi ureditev povezovanja zbirk v javnem sektorju, ki pred izvedbo zahteva oceno učinka in posvet z nadzornim organom. Poleg tega tako uvaja dnevnike obdelav, ki omogočajo sledljivost in nadzor – obvezni so zlasti pri obsežnih obdelavah posebnih vrst podatkov ali sistematičnem spremljanju posameznikov (Kovačevič, 2023).

ZVOP-2 določa tudi pogoje za imenovanje pooblaščene osebe za varstvo podatkov – obvezno za določene organizacije, drugod je to prostovoljno. Pooblaščenci imajo svetovalno in nadzorno vlogo ter morajo biti strokovno usposobljeni (Kovačevič, 2023). Na področju biometrije zakon omejuje uporabo na zakonsko utemeljene primere, medtem ko videonadzor zahteva razširjeno obvestilo posamezniku in je na javnih površinah dovoljen le ob resni nevarnosti za ljudi ali premoženje, pri čemer mora biti obdelava podatkov sledljiva (Kovačevič, 2023).

3.2.1 Zagotavljanje varstva osebnih podatkov

V 22. členu ZVOP-2 je določeno, da je za zagotavljanje varne obdelave osebnih podatkov v določenih primerih obvezno vodenje dnevnika obdelav. To velja zlasti pri obsežni obdelavi posebnih vrst podatkov, sistematičnem spremljanju posameznikov ali kadar ocena učinka pokaže povečano tveganje. Dnevnik beleži vrsto obdelave, datum, čas, izvajalca in uporabnike podatkov. Namenjen je nazoru, zagotavljanju varnosti in odpravi morebitnih napak. Podatki iz dnevnika se hranijo dve leti, v določenih primerih tudi do pet let (22. člen ZVOP-2). Za informacijske sisteme, ki obdelujejo občutljive podatke – denimo zdravstvene, kazenske ali podatke več kot 100.000 posameznikov –, veljajo dodatne varnostne zahteve. Ti sistemi morajo preprečiti uničenje, nepooblaščen dostop in nezakonite spremembe, ki bi lahko ogrozile interese države. Obdelava biometričnih, zdravstvenih in kazenskih podatkov mora potekati znotraj znanih lokacij v Sloveniji – hranjenje v tujini ni dovoljeno (23. člen ZVOP-2).

24. člen ZVOP-2 določa, da je ocena učinka na varstvo podatkov obvezna pri uvajanju posebnih vrst obdelav ali spremembi njihove pravne podlage. Ugotavlja morebitne negativne vplive, zlasti na varnost države. Ob pripravi zakona, ki ureja takšne obdelave, mora predlagatelj priložiti oceno učinka in pridobiti mnenje nadzornega organa. Kadar ocena učinka ni obvezna, je zadosten predhodni posvet. Ocena učinka mora biti dostopna nadzornim organom, Varuhu človekovih pravic in drugim pristojnim institucijam (24. člen ZVOP-2).

V skladu s 43. členom ZVOP-2 mora biti rok hrambe podatkov omejen na najkrajše obdobje, ki je potrebno za dosego namena obdelave, razen če zakon določa drugače. Upravljavec mora redno in dokumentirano preverjati, ali so roki hrambe še ustrezni glede na vrsto podatkov in tveganja. Ko je namen dosežen, je treba podatke izbrisati, uničiti, anonimizirati ali kako drugače obdelati tako, da posameznika, iz teh podatkov, ni več mogoče prepoznati

– na primer z arhiviranjem, blokado ali omejitvijo dostopa, če ni predpisano drugače (43. člen ZVOP-2).

ZVOP-2 v 46. členu določa pogoje imenovanja pooblaščene osebe za varstvo osebnih podatkov. Gre za neodvisnega strokovnjaka, ki upravljavcem in obdelovalcem pomaga pri zagotavljanju skladnosti z zakonodajo (44. člen ZVOP-2). Njeno imenovanje je obvezno za javni sektor in za tiste, ki obdelujejo občutljive podatke, drugi pa to lahko storijo prostovoljno (45. člen ZVOP-2). Oseba mora biti strokovno usposobljena, zanesljiva in brez nasprotij interesov (46. člen ZVOP-2). Njene naloge vključujejo oceno tveganj, svetovanje in skrb za varnost podatkov, pri čemer nora varovati zaupnost (48. člen ZVOP-2). Možno je tudi imenovanje namestnika ali skupne pooblaščene osebe za več upravljavcev (45. člen ZVOP-2). Pooblaščena oseba in njen namestnik sta dolžna varovati tajnost obdelovanih osebnih podatkov tako med opravljanjem nalog kot po njegovem zaključku, pridobljene informacije pa lahko uporabljata izključno za namen svojega dela (50. člen ZVOP-2).

Uporaba biometrije v trženjske ali druge komercialne namene ni dovoljena, tudi če so povezane storitve za uporabnika brezplačne (84. člen ZVOP-2).

3.2.2 Videonadzor ter evidentiranje vstopov in izstopov iz službenih prostorov

V 76. členu ZVOP-2 je določeno, da lahko videonadzor izvajajo javni in zasebni upravljavci, če za to obstajajo utemeljeni razlogi, določeni s pisno odločitvijo. Posamezniki morajo biti o snemanju jasno obveščeni, posnetki pa se lahko hranijo največ eno leto, razen če zakon določa drugače. V javnem prometu je rok hrambe sedem dni, na javnih površinah pa šest mesecev. Videonadzor je prepovedan v prostorih, kjer se pričakuje večja zasebnost, kot so sanitarije, garderobe ali hoteli (76. člen ZVOP-2).

V poslovnih prostorih je nadzor dovoljen zaradi varnosti ljudi, premoženja ali kontrole dostopa, vendar ne sme posegati v zasebne dele stanovanjskih stavb. Zaposleni morajo biti o tem obveščeni, zbirka pa lahko vsebuje le osnovne osebne podatke in podatke o dostopu v prostore (77. člen ZVOP-2). Na delovnem mestu je snemanje dopustno le, če je nujno zaradi varnosti ali preprečevanja kršitev, nikoli pa na delovnem mestu zaposlenega, razen ob izjemni nujnosti. Pred uvedbo mora delodajalec opraviti posvet z zaposlenimi in s sindikatom (78. člen ZVOP-2). V javnem prometu in na javnih površinah je videonadzor dovoljen le, če z milejšimi ukrepi ni mogoče zagotoviti varnosti. Posnetke je dovoljeno hraniti največ sedem dni v prometu in šest mesecev na javnih površinah, uporaba biometrije, samodejnega prepoznavanja registrskih tablic ali sistematičnega sledenja pa je prepovedana (79. člen ZVOP-2). Upravljavci morajo zagotoviti varnost opreme in sledljivost obdelave, pri čemer se vsi vpogledi in prenosi beležijo v dnevnik, ki se hrani dve leti po zaključku obdelave (76. člen ZVOP-2).

Evidentiranje vstopov in izstopov iz službenih prostorov je dovoljeno zaradi varnosti, varovanja tajnih podatkov in zagotavljanja reda. Zbirajo se lahko osnovni podatki

obiskovalca, kot so ime, dokument, zaposlitev, vozilo, čas in namen obiska. Podatki se hranijo največ dve leti, razen če zakon določa drugače (85. člen ZVOP-2).

3.2.3 Obdelava biometričnih in genskih podatkov

Po 81. členu ZVOP-2 je obdelava biometričnih in genskih podatkov dovoljena le, če za to obstaja zakonska podlaga ali če posameznik poda izrecno privolitev. Povezovanje biometričnih zbirk z drugimi zbirkami ni dovoljeno, razen, če zakon ali soglasje posameznika določata drugače. Genske podatke je dovoljeno obdelovati le za zdravstvene namene ali na podlagi posebnih pogodb, ki koristijo posamezniku (81. člen ZVOP-2).

82. člen ZVOP-2 pravi, da je v javnem sektorju uporaba biometrije dovoljena le, če je nujno potrebna za varnost ljudi, zaščito premoženja, varovanje tajnih podatkov ali identifikacijo pogrešanih oseb. Izjeme vključujejo mejne prehode, izdajo elektronskih identitet in izpolnjevanje mednarodnih obveznosti. Uporaba biometrije za vstop v javne stavbe je dopustna le, če druge rešitve niso učinkovite (82. člen ZVOP-2).

Skladno s 83. členom ZVOP-2 je v zasebnem sektorju uporaba biometričnih podatkov mogoča le, če je nujna za izvajanje dejavnosti ali zaščito občutljivih informacij, in sicer na podlagi zakona, pogodbe ali izrecne privolitve. Vedno mora biti na voljo alternativna možnost identifikacije brez uporabe biometrije. Običajno je potrebno predhodno dovoljenje nadzornega organa, razen v izjemnih primerih. Zaposleni morajo biti pisno obveščeni, obdelava pa mora biti sorazmerna (83. člen ZVOP-2).

3.2.4 Kazenske določbe

Kot določa 95. člen ZVOP-2, kazenske določbe tega zakona urejajo sankcije za kršitve uredbe GDPR in nacionalnih predpisov. Globe se izrekajo pravnim osebam, samostojnim podjetnikom, posameznikom z dejavnostjo in odgovornim osebam. Njihova višina je odvisna od narave, teže in okoliščin kršitve (95. člen ZVOP-2).

Zakon predvideva denarne kazni za kršitve temeljnih načel varstva osebnih podatkov, pravic posameznikov, obveznosti upravljavcev in izvajanje nadzora brez zakonske podlage. Strožje kazni veljajo za hujše kršitve, kot sta neupravičeno snemanje na mestih z večjo zasebnostjo (npr. sanitarije, hotelske sobe) ali zloraba biometričnih podatkov. Višina glob za pravne osebe lahko doseže do 40.000 evrov, za samostojne podjetnike do 10.000 evrov, za odgovorne osebe do 5.000 evrov in za posameznike do 2.000 evrov. Posebej so sankcionirane zlorabe videonadzora, obdelava biometričnih in genskih podatkov brez ustrezne pravne podlage ter neustrezno varovanje sistemov. Uporaba teh podatkov v trženjske namene je strogo prepovedana. Upravljavci morajo spoštovati roke hrambe in vzpostaviti varnostne ukrepe, v nasprotnem primeru so lahko kaznovani (96.–113. člen ZVOP-2).

Pri odmeri globe nadzorni organ upošteva, ali je bila kršitev namerna, ali so bili sprejeti popravljalni ukrepi, ali je šlo za ponavljajoče se ali množične kršitve in ali je kršitelj samoiniciativno ukrepal. Prav tako se upošteva finančno stanje posameznikov v sorazmernosti sankcije (114. člen ZVOP-2). Globe se lahko izrečejo tudi v hitrem postopku, nad minimalno predpisanimi zneski (115. člen ZVOP-2).

3.3 Informacijski pooblaščenec

Zakon o Informacijskem pooblaščencu (ZInfP) Uradni list RS, št. 113/05 in 51/07 – ZUstS-A ureja ustanovitev in delovanje Informacijskega pooblaščenca kot samostojnega in neodvisnega državnega organa. Ta varuje pravico do zasebnosti in dostopa do informacij javnega značaja ter uresničuje določbe evropske Direktive 95/46/ES o varstvu osebnih podatkov (1. člen ZInfP). Leta 2024 je bila na mesto vodje Informacijskega pooblaščenca predlagana in izvoljena pooblaščenka Jelena Virant Burnik (IPRS, 2025b).

Informacijski pooblaščenec je pristojen za odločanje o pritožbah glede dostopa do informacij javnega značaja, za inšpekcijski nadzor nad obdelavo osebnih podatkov in za reševanje pritožb posameznikov, kadar upravljavec ne izpolni njihovih pravic do lastnih osebnih podatkov (2. člen ZInfP). Poleg tega ima Informacijski pooblaščenec tudi prekrškovna pooblastila in vodi strokovno službo (9. člen ZInfP), skrbi za organizacijo dela in opravlja naloge predstojnika državnega organa (2. člen ZInfP). Sredstva za njegovo delovanje se zagotavljajo iz državnega proračuna, njihovo višino pa na predlog pooblaščenca določi državni zbor (5. člen ZInfP). Imenovanje pooblaščenca poteka v pristojnosti Državnega zbora na predlog predsednika Republike Slovenije, in sicer za petletni mandat z možnostjo ponovnega imenovanja. Kandidat mora biti državljan Slovenije, imeti univerzitetno izobrazbo, vsaj pet let izkušenj in ne sme biti kazensko obsojen (6. člen ZInfP).

V postopkih nadzora in reševanja pritožb ima pooblaščenec pravico zahtevati dokumentacijo od organov, tudi če gre za davčne informacije, če so pomembne za obravnavo zadeve. Če organ ne sodeluje, lahko pooblaščenec ukrepa z inšpekcijskimi pooblastili. Upravni spori v teh primerih so nujni in imajo prednost (10. člen ZInfP). Informacijski pooblaščenec mora vsako leto do 31. maja pripraviti in objaviti poročilo o svojem delu, v katerem poda tudi oceno in priporočila glede varstva osebnih podatkov in dostopa do informacij javnega značaja (14. člen ZInfP). Za nespoštovanje odločb in neizpolnjevanje obveznosti v postopku se odgovorne osebe kaznujejo z denarno globo, zlasti če ne posredujejo zahtevanih dokumentov ali ne omogočijo uresničitve pravic posameznikov (15. člen ZInfP).

4 VARSTVO OSEBNIH PODATKOV V RAČUNOVODSTVU

Računovodstvo vključuje obdelavo številnih osebnih podatkov, predvsem zaradi izpolnjevanja zakonskih zahtev. Posledično se računovodje pogosto ne zavedajo vseh tveganj, povezanih s tem področjem. S sprejetjem GDPR je maja 2018 prišlo do pomembnih

sprememb, ki so povečale odgovornost organizacij in okrepile pravice posameznikov (Bajuk Mušič, 2018). GDPR velja za vse organizacije, ki obdelujejo osebne podatke, torej tudi za računovodske servise. Ti morajo jasno opredeliti svojo vlogo – ali nastopajo kot upravljavci ali obdelovalci (ICAEW, 2018). Obdelava osebnih podatkov po GDPR pomeni katero koli dejanje z osebnimi podatki – od zbiranja, urejanja, shranjevanja do izbrisa (Bajuk Mušič, 2018).

Po Bajuk Mušič (2018) računovodski servisi obdelujejo podatke o vseh poslovnih dogodkih organizacije, pri čemer osebni podatki predstavljajo le del tega obsega. Vrsta in količina obdelovanih osebnih podatkov se razlikujeta glede na dejavnost organizacije. Če organizacija obdelavo osebnih podatkov zaupa zunanjim izvajalcem, na primer pri obračunu plač, to ne pomeni, da je oproščena odgovornosti za skladnost z GDPR. V tem primeru organizacija nastopa kot upravljavec osebnih podatkov, računovodski servis pa kot obdelovalec. Upravljavec ne more prenesti svoje odgovornosti na obdelovalca, ampak sta oba dolžna zagotavljati varnost in skladnost obdelave. Teehan (2025) nadaljuje, da morajo računovodski servisi, ker obdelujejo tudi podatke o dobaviteljih in strankah naročnika, vzpostaviti ustrezne varnostne politike: varna gesla, šifriranje, zaščitene portale, varnostne kopije in postopke prijave kršitev. Pomembno je tudi, da zagotovijo hrambo podatkov znotraj Evropskega gospodarskega prostora in to jasno določijo v pogodbah. Čeprav so kazni za kršitve visoke, je varno ravnanje z osebnimi podatki že dolgo del dobre računovodske praske.

Ključno merilo pri razmejitvi vlog je, kdo določa namen in sredstva obdelave podatkov. Če to dela naročnik, računovodski servis nastopa kot pogodbeni obdelovalec. Upravljavec je odgovoren za ustrezne pogodbe in skladnost z zakonodajo, obdelovalec pa mora podatke obdelovati izključno v okviru pooblastil naročnika in skladno z GDPR (IPRS, 2020). Za računovodske servise GDPR pomeni trajno vključevanje zaščite osebnih podatkov v vsakodnevno delo – ne gre le za enkraten postopek. Med ključnimi obveznostmi so: vodenje dokumentacije, pridobivanje jasne privolitve, upoštevanje pravice do izbrisa, prijava kršitev nadzornemu organu, presoja učinkov na zasebnost, posodobitev pogodb in politik zasebnosti ter zagotovitev skladne programske opreme (Thomson Reuters Tax and Accounting, 2018).

Bajuk Mušič (2018) zaključuje, da je GDPR namenjena zaščiti morebitnih osebnih podatkov fizičnih oseb. Tako upravljavec kot obdelovalec sta odgovorna za varstvo teh podatkov in morebitne kršitve. Če pride do kršitve varstva osebnih podatkov in posledične škode, sta odgovorna posamezniku, pri čemer te odgovornosti ni mogoče omejiti ali prenesti.

4.1 Obdelava osebnih podatkov v računovodstvu

Po Bajuk Mušič (2018) ZRFR priporoča, da računovodstva evidentirajo vrste osebnih podatkov, ki jih obdelujejo, vključno s tistimi, ki jih hranijo v arhivu. Nekaj podobnega bi morala računovodstva že opredeliti v okviru izvirnih in izvedenih knjigovodskih in poslovnih knjig. Vendar osebni podatki, ki jih organizacije zbirajo za obračune plač, ne

sodijo neposredno med knjigovodske listine ali poslovne knjige. Nadaljuje, da se osebni podatki pogosto nahajajo na dokumentih, ki služijo kot podlaga za knjiženje, zato je pri določanju vrste osebnih podatkov pomembno upoštevati ne le popis knjigovodskih listin, temveč tudi celoten krogotok poslovnih procesov dogodkov in stanj. Računovodstvo obdeluje predvsem osebne podatke zaposlenih, še posebej kadar kadrovska služba deluje znotraj računovodstva in ni ločen oddelek. Sem sodijo kadrovske evidence ter drugi podatki, potrebni za obračun plač, davkov, prispevkov in drugih odtegljajev. Dodaja, da organizacija obdeluje osebne podatke posameznikov, ki z njo sodelujejo kot pogodbeni izvajalci – na primer na podlagi avtorskih in podjemnih pogodb, pogodb upokojencev, ki opravljajo začasno ali občasno delo, ter drugih fizičnih oseb, s katerimi ima kasneje sklenjene pogodbe. Osebni podatki se pojavljajo tudi na izdanih računih, ki so naslovljeni na fizične osebe kot kupce.

Organizacija lahko podatke obdeluje le zakonito in za vnaprej določene namene. Njihova kasnejša uporaba za druge namene ni dovoljena. Podatki morajo biti ustrezni, ažurni in zgolj za namen, za katerega so bili pridobljeni. Poudarja, da je v računovodstvu obdelava osebnih podatkov najpogosteje povezana z izpolnjevanjem zakonskih obveznosti. To vključuje zbiranje podatkov za prijavo in odjavo zaposlenih, obračun prispevkov in davkov, uveljavljanje olajšav za vzdrževane družinske člane ter podobne postopke. Pojasnjuje, da je obdelava osebnih podatkov lahko potrebna tudi za izvajanje pogodbe, na primer pri pripravi obračuna kapitalskega dobička. S privolitvijo se računovodstvo običajno ne srečuje pogosto, lahko pa opozori na morebitne kršitve varstva osebnih podatkov. Ena izmed takšnih je, da je na izdanem računu fizična osebna navedena z imenom, s priimkom, z naslovom, elektronskim naslovom ali s telefonsko številko – v takem primeru gre za obdelavo osebnih podatkov (Bajuk Mušič, 2018).

Bajuk Mušič (2018) opozarja, da GDPR obravnava osebne podatke skozi štiri faze življenjskega cikla: zbiranje in ustvarjanje podatkov, uporaba in obdelava, hramba in arhiviranje ter izbris in uničenje. Družba mora imeti vzpostavljen nadzor nad osebnimi podatki skozi celotno življenjsko dobo njihove obdelave. Dodaja, da se podatki lahko hranijo le, dokler obstaja zakonita podlaga za njihovo obdelavo. Če so bili podatki zbrani na podlagi soglasja, jih lahko hrani le do izpolnitve namena ali do preklica soglasja. Po tem jih mora fizično uničiti. V primeru elektronske hrambe mora poskrbeti, da jih ni več mogoče obnoviti. Nadaljuje, da je za računovodstvo ključno, da najprej identificira, katere osebne podatke obdeluje in ali za njihovo obdelavo obstaja zakonska podlaga ali potrebuje privolitev. Nato mora določiti rok hrambe za vsako vrsto podatkov in poskrbeti, da se ti roki dosledno upoštevajo. Osebne podatke smejo obdelovati le zaupanja vredne osebe, ki so zavezane k varovanju zaupnosti.

4.1.1 Hramba in evidenca obdelave osebnih podatkov

Kraigher Mišič (2019) poudarja, da je pri določanju rokov hrambe dokumentacije treba upoštevati namen hrambe, vsebino poslovanja, zakonodajo in dejavnost organizacije. V računovodstvu so zakonsko določeni roki hrambe praviloma minimalni, vendar pri dokumentaciji z osebnimi podatki hkrati predstavljajo tudi najdaljše dovoljeno obdobje hrambe. Hramba osebnih podatkov mora biti skladna z zakonodajo, zato morajo družbe, med katere sodijo tudi računovodski servisi, vnaprej določiti pravno podlago obdelave, trajanje hrambe in ukrepe za varovanje podatkov. Čas hrambe je odvisen od pravne podlage. Dodaja tudi, da so poleg zakonitosti ključni tudi ustrezna fizična in tehnična zaščita podatkov ter zagotavljanje sledljivosti dostopov. Po 30. členu ZR se knjigovodske listine in poslovne knjige v računovodstvu hranijo v skladu z veljavnimi predpisi, pri čemer so določeni minimalni roki hrambe glede na vrsto dokumentacije. Trajno se hranijo letni računovodski izkazi, končni obračuni plač zaposlenih in izplačilne liste za tista obdobja, za katera končni obračuni plač niso bili izdelani. Dokumentacija, kot sta glavna knjiga in dnevnik, se mora hraniti najmanj deset let. Knjigovodske listine, ki so podlaga za knjiženje, z zakonom predpisane listine in pomožne knjige se hranijo pet let. Knjigovodske listine, povezane s plačilnim prometom, se hranijo najmanj tri leta. Najkrajši rok hrambe, to je dve leti, velja za prodajne in kontrolne bloke ter pomožne obračune in podobne knjigovodske listine.

Bajuk Mušič (2018) ugotavlja, da računovodskim servisom, ki obračunavajo plače za manjše organizacije, evidence ni treba voditi. Drugače je, če servis obdeluje podatke za organizacije z več kot 250 zaposlenimi. V takem primeru mora upravljavec (organizacija) voditi splošno evidenco obdelave, v katero so vključene tudi dejavnosti obdelave obdelovalcev, kot je računovodski servis. Poudarja, da je evidenca dejavnosti obdelave interna dokumentacija in je ni treba pošiljati nadzornim organom. Kljub temu ZRFR priporoča, da jo vodijo tudi manjše organizacije, saj omogoča boljši vpogled v obdelavo osebnih podatkov in vzpostavitev učinkovitejših varnostnih mehanizmov.

4.1.2 Zagotovitev tehničnih in organizacijskih ukrepov za zaščito osebnih podatkov

Po Bajuk Mušič (2018) družba mora sama presoditi, ali nastopa v vlogi upravljavca ali obdelovalca osebnih podatkov, pri čemer mora upoštevati način in vrsto obdelave. Upravljavec je tisti, ki sam ali skupaj z drugimi določa namene in sredstva obdelave podatkov – stranka, medtem ko obdelovalec podatke obdeluje izključno v skladu z navodili upravljavca – računovodski servis. GDPR na podlagi namena obdelave natančno določa obveznosti obeh.

Bajuk Mušič (2018) poudarja, da mora upravljavec zagotoviti in izvesti ustrezne tehnične organizacijske ukrepe ter dokazati, da obdelava poteka v skladu s predpisi. Če pri obdelavi uporablja storitve obdelovalca, kot je na primer računovodski servis, mora poskrbeti za dokumentirane postopke in preverjati njihovo izvajanje. S tem prevzema odgovornost za izbiro ustreznega obdelovalca. Posledično trdi, da so organizacije, ki uporabljajo storitve

računovodskih servisov – zlasti večja podjetja –, postale zahtevnejše in pogosto zahtevajo skladnost s kodeksi ali z drugimi pravili dobre prakse. Upravljavec in obdelovalec morata za vsako vrsto ali sklop osebnih podatkov določiti tehnične in organizacijske zahteve. Tehnični ukrepi vključujejo omejevanje dostopa revizijske sledi in druge varnostne mehanizme. Organizacijski ukrepi pa določajo, kdo sme in kdo ne sme dostopati do podatkov in kako jih lahko uporablja. Na primer v računovodskem servisu ne more vsak zaposleni dostopati do modula za obračun plač ali do pogodb o zaposlitvi, saj so ti podatki zaščiteni z gesli.

V praksi se pogosto zgodi, da je osebne podatke treba posredovati tretjim osebam, kot so inšpekcijski organi. Vendar upravljavec in obdelovalec ne smeta hraniti osebnih podatkov zgolj za morebitne prihodnje inšpekcijske preglede. Podatke, ki niso več potrebni za prvotni namen zbiranja, je treba trajno izbrisati ali uničiti. Enako velja, če posameznik prekliče soglasje za njihovo obdelavo. Izjema so primeri, ko je obdelava potrebna zaradi zakonitih dejavnosti upravljavca, vendar morebitni inšpekcijski pregledi v to kategorijo ne spadajo. Upravljavec mora v takšnih primerih dokazati, da je njegov zakoniti interes močnejši od interesov posameznika, na katerega se osebni podatki nanašajo (Bajuk Mušič, 2018).

4.1.3 Pogodbeno razmerje med upravljavcem in obdelovalcem

Bajuk Mušič (2018) navaja, da GDPR jasno določa zahteve, ki jih mora vsebovati pogodba med upravljavcem in obdelovalcem, pri čemer so v primeru računovodskih storitev upravljavci osebnih podatkov stranke, obdelovalci pa računovodski servisi. Nadaljuje, da primarno odgovornost za zakonito obdelavo osebnih podatkov nosi stranka, vendar sta tako računovodski servis kot tudi stranka skupaj odgovorna posameznikom, katerih podatke obdelujeta. Zaradi te skupne odgovornosti morajo stranke pri izbiri računovodskega servisa zagotoviti, da ta deluje skladno z GDPR.

Stranka kot upravljavec je odgovorna za določitev in izvajanje ustreznih organizacijskih in tehničnih ukrepov za varovanje osebnih podatkov, računovodski servis pa jih mora pri obdelavi ustrezno upoštevati. Nadaljuje, da ti ukrepi vključujejo omejevanje dostopa do osebnih podatkov, zaščito elektronskih podatkov z gesli ter zagotavljanje revizijske sledi za vse dostope in spremembe. Prav tako trdi, da je raven zaščite odvisna od narave in občutljivosti podatkov in okoliščin obdelave. Računovodski servis brez soglasja stranke ne sme vključiti drugega obdelovalca, kar se v praksi lahko zgodi pri primeru obračuna plač, ko zaposleni, ki izvaja obdelavo, zboli in bi morala nalogo prevzeti zunanja oseba. Brez posebnega dovoljenja takšna predaja dela ni dovoljena, razen če pogodba določa splošno soglasje, pri čemer pa mora računovodski servis stranko obvestiti o spremembi (Bajuk Mušič, 2018).

Bajuk Mušič (2018) trdi, da morajo biti v pogodbah o izvajanju storitev, ki vključujejo obdelavo osebnih podatkov, določene ključne zahteve. Računovodski servis mora podatke obdelovati zgolj po navodilih stranke, zagotoviti zaupnost oseb, ki obdelujejo podatke, in

upoštevati varnostne ukrepe iz 32. člena GDPR. Navaja, da mora prav tako spoštovati pogoje glede vključevanja drugih obdelovalcev, pomagati stranki pri izpolnjevanju obveznosti do posameznikov in po koncu pogodbenega razmerja podatke bodisi izbrisati ali vrniti stranki. Poleg tega mora računovodski servis omogočiti nadzor nad izvajanjem ukrepov in revizijske preglede. Preprosto povedano, obdelovalec se mora zavezati k enakim standardom varstva osebnih podatkov, kot jih zagotavlja upravljavec (Bajuk Mušič, 2018).

4.1.4 Obdelava osebnih podatkov pri računovodstvu v oblaku

Po La Torre in drugi (2021) digitalna preobrazba – predvsem big data in z njimi povezane tehnologije – pomenljivo vplivajo na vlogo računovodij in revizorjev, pri čemer se varstvo osebnih podatkov izkaže kot nova šibka točka. Napredek na podlagi računalništva v oblaku je povzročil spremembe tudi v računovodstvu. Moudud-Ul-Huq in drugi (2020) navajajo, da je bilo s pojavom novih tehnologij na trgu in z vse večjo digitalizacijo poslovanja pričakovano, da se bo tudi opravljanje računovodskih storitev premaknilo v oblak. Khanom (2017) meni, da je računovodstvo v oblaku sodobna oblika računovodstva, ki temelji na uporabi oblačne tehnologije za shranjevanje, obdelavo in dostop do finančnih podatkov prek interneta. Moudud-Ul-Huq in drugi (2020) nadaljujejo, da ključne prednosti njegove uporabe vključujejo večjo varnost podatkov, saj so ti shranjeni na več oddaljenih strežnikih in zaščiteni s šifriranjem, povečano produktivnost zaradi avtomatizacije ponavljajočih se nalog, prihranek stroškov, saj ni potrebe po lastni IT-infrastrukturi, ter stalni dostop do podatkov od kjer koli in kadar koli (Moudud-Ul-Huq in drugi, 2020). Kljub številnim prednostim obstajajo tudi številna tveganja, med katerimi so vdor v podatke (Abdalla in Varol, 2019), notranje grožnje zaradi dostopa zaposlenih (Moudud-Ul-Huq in drugi, 2020), odvisnost od internetne povezave (Lavinski, 2019) in težave pri integraciji z že obstoječimi poslovnimi sistemi (Moudud-Ul-Huq in drugi, 2020).

Bajuk Mušič (2018) še dodaja, da sta pravilna izbira ponudnika in ustrezna zaščita podatkov tako ključnega pomena za varno in učinkovito uporabo računovodstva v oblaku. Nadaljuje, da pri računovodenju v oblaku GDPR velja ne glede na fizično lokacijo strežnikov, ključno pa je, kje poteka obdelava osebnih podatkov in katera zakonodaja lahko nanjo vpliva. Ponudnik oblačnih storitev ima v tem primeru vlogo obdelovalca, zato mora upravljavec zagotoviti, da ta izpolnjuje zahteve GDPR, tudi kadar zaposleni uporabljajo zunanje aplikacije za hrambo ali izmenjavo podatkov. Poudarja, da je za varnost osebnih podatkov, tudi v oblaku, odgovoren upravljavec, ki mora izbrati ponudnika z ustreznimi tehničnimi in organizacijskimi ukrepi ter biti sposoben dokazati, da so bili sprejeti vsi razumni varnostni ukrepi.

4.2 Izzivi, prednosti in uporaba splošne uredbe v računovodstvu

Varstvo osebnih podatkov je, zlasti po uvedbi GDPR, v računovodstvu postalo osrednji vidik dela. Vloga računovodij se lahko glede na njihovo naravo dela spreminja. Pri izvajanju

storitev za stranke (upravljavce), ki nimajo samostojnega vpliva na namen obdelave, nastopajo kot obdelovalec podatkov. V tem primeru mora računovodski servis s stranko skleniti pogodbo o obdelavi osebnih podatkov (Bodnarova, 2019), zanj pa veljajo vse zahteve, ki jih GDPR določa za obdelovalce (Bajuk Mušič, 2018). Bodnarova (2019) izpostavlja, da kljub temu obstaja izjema, kadar računovodje odkrijejo nepravilnosti pri obdelavi osebnih podatkov, ki jih morajo prijaviti. Takrat ravnajo kot samostojni upravljavci podatkov, saj delujejo neodvisno in v skladu z zakonskimi obveznostmi.

Stanciu in Rîndașu (2018) menita, da se morajo računovodski servisi predvsem osredotočiti na tri ključna področja: (1) jasno določitev pravne podlage za obdelavo osebnih podatkov (npr. pogodba, zakonska obveznost), (2) zagotavljanje pravic posameznikov (pravica do dostopa, popravka, izbrisa, omejitve obdelave ipd.) in (3) uvedbo varnostnih mehanizmov v okviru informacijskih sistemov, kot so šifriranje, anonimizacija in odstop na podlagi pooblastil (Stanciu in Rîndașu, 2018).

Bajuk Mušič (2018) poudarja, da mora računovodski servis najprej jasno določiti, katere osebne podatke obdeluje ter upravljavcu zagotoviti ustrezno pomoč in podporo. Če za obdelavo osebnih podatkov uporablja storitve v oblaku, mora pridobiti posebno soglasje upravljavca, torej stranke, in ga obveščati o morebitnih spremembah. Dodaja še, da mora poleg tega vzpostaviti proces za posredovanje podatkov na zahtevo posameznika ter zagotoviti ustrezne postopke za brisanje in uničenje podatkov, ko ti niso več potrebni. Pri elektronski obdelavi podatkov je ključnega pomena tudi revizijska sledljivost, ki omogoča nadzor nad vpogledi, spremembami in drugimi obdelavami osebnih podatkov. Nato mora računovodski servis vzpostaviti tudi ustrezne tehnične in organizacijske ukrepe za varstvo osebnih podatkov. Obdelava mora potekati na podlagi dokumentiranih navodil, ki natančno določajo postopek ravnanja z osebnimi podatki.

4.2.1 Uporabnost, izzivi in prednosti uvedbe zahtev splošne uredbe v manjših podjetjih

Tudi mikro in majhna podjetja, ki pri poslovanju uporabljajo spletna orodja in obdelujejo osebne podatke strank ali zaposlenih, morajo izpolnjevati temeljne zahteve GDPR, kot so določitev pravnih podlag obdelave, vodenje evidence dejavnosti obdelave, pridobivanje veljavnih soglasij, priprava politik zasebnosti in sklenitev pogodb z zunanjimi obdelovalci. Posebno pozornost je treba nameniti preglednosti obdelave na spletnih straneh, upravljanju piškotkov in varovanju občutljivejših oblik obdelave, kjer so lahko potrebne dodatne ocene tveganj (Data d. o. o., 2025). Delodajalci morajo sprejeti ustrezne interne akte in zaposlene seznaniti z varstvom osebnih podatkov (Data d. o. o., 2024). Ker so sankcije za kršitve lahko visoke ne glede na velikost podjetja, ustrezna ureditev varstva osebnih podatkov ni le zakonska obveznost, temveč tudi pomemben dejavnik zaupanja, zmanjševanja tveganj in dolgoročne poslovne uspešnosti (Data d. o. o., 2025).

Xuereb, in drugi (2019) menijo, da za manjša računovodska podjetja ali samostojne računovodske servise predstavlja skladnost z GDPR poseben izziv. Ta podjetja pogosto

nimajo specializiranega kadra, kot so strokovnjaki za informacijsko varnost ali pravniki, ki bi jim pomagali pri pravilni interpretaciji in implementaciji uredbe. Zato se pogosto zanašajo na zunanje svetovalce, kar pomeni dodatne stroške, ki jih težje prenesejo kot večje organizacije. Poleg kadrovskih omejitev kot težavo vidijo tudi tehnične vire. Manjša podjetja morda uporabljajo starejšo programsko opremo ali cenejše rešitve, ki nimajo vgrajenih funkcionalnosti za varno obdelavo osebnih podatkov, kot so šifriranje, revizijske sledi ali samodejna anonimizacija. Prav tako pogosto nimajo oblikovanih notranjih politik varstva podatkov, protokolov za obvladovanje morebitnih kršitev ali načrtov za obvladovanje tveganj. Poudarjajo, da sta zanje lahko obremenjujoča tudi spremljanje pravnih sprememb in redno posodabljanje dokumentacije (npr. politike zasebnosti, pogodbe o obdelavi podatkov, interni pravilniki). Poleg tega nimajo vedno jasnega vpogleda v vlogo, ki jo imajo kot upravljavci ali obdelovalci osebnih podatkov – napačna ocena pa lahko vodi do pravne odgovornosti. Dodajajo, da ne gre spregledati tudi časovne obremenitve – izvajanje vseh nalog, povezanih z GDPR (evidenca dejavnosti obdelave, upravljanje zahtev posameznikov, poročanje o kršitvah), dodatno obremenjuje že tako omejene resurse manjših pisarn. Zaradi vsega navedenega se ta podjetja znajdejo v precej negotovem položaju, pri čemer je tveganje za nenamerno neskladnost z zakonodajo bistveno večje (Xuereb in drugi, 2019).

Kljub izzivom Xuereb in drugi (2019) poudarjajo, da GDPR predstavlja tudi pomembno priložnost – še posebej za manjše računovodske organizacije –, da okrepijo zaupanje svojih strank. Stranke v današnjem digitalnem okolju postajajo vse bolj ozaveščene o pomenu varstva osebnih podatkov in pogosto pričakujejo visoko raven odgovornosti pri ravnanju z njihovimi informacijami. Ugotavljajo, da če računovodski subjekt transparentno komunicira, kako ravna z osebnimi podatki, in pokaže jasno zavezanost k varnosti in zasebnosti, si lahko s tem bistveno okrepi ugled. Upoštevanje GDPR po njihovem mnenju ne pomeni le zakonodajne skladnosti, temveč daje priložnost za profesionalizacijo poslovanja. Uredba spodbuja uvedbo standardiziranih, preglednih in varnih postopkov, kar ima tudi notranje koristi: boljši nadzor nad podatki, manjše tveganje za izgubo podatkov ali napake ter večjo učinkovitost pri odzivanju na zahteve strank.

Računovodska podjetja, ki vlagajo v zaščito podatkov in varne IT-rešitve, strankam dajejo jasen signal, da jim je mar za varnost in zasebnost, kar je v občutljivih panogah, kot je računovodstvo – denimo zaradi obdelave plač, davkov ali drugih osebnih finančnih podatkov –, odločilnega pomena. Dodajajo, da ima poleg tega dejavno spoštovanje GDPR dolgoročne poslovne učinke: zvestoba strank, večje možnosti pridobivanja novih strank, ki iščejo zanesljivega ponudnika storitev in boljše konkurenčne prednosti na trgu. V tem smislu je uredba več kot le pravna obveznost, je tudi orodje za dvig kakovosti, odgovornosti in zaupanja v storitve, ki jih računovodstvo nudi (Xuereb in drugi, 2019).

4.3 Zakon o preprečevanju pranja denarja in financiranja terorizma v računovodstvu ter varstvo osebnih podatkov

Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-2) Uradni list RS, št. 48/22, 145/22 in 17/25 določa obveznosti za zavezance – med njimi tudi računovodske servise – z namenom preprečevanja zlorab finančnega sistema. Hkrati zakon ureja tudi obdelavo osebnih podatkov, ki jih ti subjektu zbirajo in hranijo pri izvajanju svojih zakonskih nalog (17. člen ZPPDFT-2).

Računovodski servisi morajo kot zavezanci ob upoštevanju določil ZPPDFT-2 izvajati vrsto ukrepov, kot so ocena tveganj, identifikacija strank, spremljanje transakcij, poročanje sumljivih dejavnosti, usposabljanje zaposlenih in vodenje evidenc. Čeprav lahko del nalog izvajajo zunanji izvajalci, zakon jasno določa, da za skladnost ostaja odgovoren zavezanec sam. To vključuje tudi ustrezno pogodbeno urejeno in zakonsko skladno obdelavo podatkov (4. člen ZPPDFT-2). Zavezanci morajo zbirati in hraniti osebne in finančne podatke svojih strank, kot so ime, priimek, naslov, EMŠO ali davčna številka, državljanstvo, podatki iz osebnih dokumentov ter informacije o transakcijah, izvoru sredstev, politično izpostavljenih osebah in dejanskih lastnikih podjetij. Vse te podatke morajo varovati v skladu s predpisi o varstvu osebnih podatkov (150. člen ZPPDFT-2).

ZPPDFT-2 določa roke hrambe: večina zbranih podatkov se mora hraniti 10 let po zaključku poslovnega razmerja ali izvedeni transakciji, podatki o usposabljanju zaposlenih pa najmanj štiri leta (142. člen ZPPDFT-2). Kopije osebnih dokumentov se praviloma uničijo po preverjanju, razen v primeru finančnih institucij, ki jih smejo hraniti v digitalni obliki do pet let, ob ustreznih varnostnih ukrepih (141. člen ZPPDFT-2). Zakon posebej poudarja tudi obveznost vodenja različnih evidenc – o transakcijah, identifikaciji strank, sumljivih dejavnostih, pooblaščencih in nadzornih postopkih. Ti podatki omogočajo nadzornim organom učinkovito preverjanje skladnosti in preprečevanje finančnih zlorab (150. člen ZPPDFT-2). Po preteku zakonskih rokov se osebni podatki izbrišejo, razen če zakon določa drugače. Ob prenehanju zavezanca se odgovornost za hrambo prenese na pristojni organ (150. člen ZPPDFT-2).

ZRFR sicer poudarja, da podatki fizičnih oseb, ki nastopajo kot predstavniki pravnih oseb (npr. direktorji, prokuristi), ne sodijo pod zaščito GDPR. Ker so ti podatki javno dostopni, jih organizacije lahko zbirajo in obdelujejo brez omejitev (Bajuk Mušič, 2018). Javno dostopni so zgolj ime, priimek in naslov prebivališča. Pri izpolnjevanju zakonskih zahtev ZPPDFT-2 morajo računovodski servisi zbrati veliko več osebnih podatkov o omenjenih osebah, ki niso javno dostopni. Gre za eno izmed pravnih podlag, nujno za izpolnjevanje zakonskih obveznosti, ki jih mora upravljavec podatkov spoštovati in je določena v 6. členu GDPR (Langeršek in Brajnik, 2018).

5 EMPIRIČNI DEL

Empirični del magistrskega dela temelji na kvalitativnem raziskovalnem pristopu, ki je bil izbran z namenom poglobljenega razumevanja skladnosti delovanja računovodskih servisov z zakonodajo o varstvu osebnih podatkov. Obravnavana tematika je kompleksna, pravno zahtevna in hkrati občutljiva, saj se nanaša na morebitne pomanjkljivosti v poslovnih praksah in neizpolnjevanje zakonskih obveznosti. Kvantitativni raziskovalni pristop v obliki anketnega vprašalnika bi v tem primeru verjetno naletel na omejitve, povezane z nizko stopnjo odzivnosti in zadržanostjo računovodskih servisov pri razkrivanju dejanskega stanja skladnosti z zakonodajo. Glede na naravo tematike obstaja utemeljena verjetnost, da bi se številni računovodski servisi izognili sodelovanju ali bi podajali družbeno zaželene odgovore, kar bi vplivalo na kakovost in verodostojnost zbranih podatkov. Zato sem se odločila za kvalitativno metodo globinskih intervjujev na manjšem, namensko izbranem vzorcu, ki je omogočila odprto, poglobljeno in vsebinsko bogato razpravo z intervjuvanci. Takšen pristop je omogočil pridobivanje realnih in podrobnih vpogledov v dejanske delovne procese, razumevanje zakonodajnih zahtev ter konkretne izzive, s katerimi se računovodski servisi soočajo v praksi.

Empirična raziskava je zasnovana tako, da v okviru kvalitativnega pristopa odgovori na ključna raziskovalna vprašanja magistrskega dela:

1. Kakšne obveznosti predpisuje trenutna zakonodaja s področja varstva osebnih podatkov računovodskim servisom?
2. Kako se predpisi s področja varstva osebnih podatkov odražajo v delovnih procesih računovodskih servisov?
3. Kakšne so posledice zahtev, ki jih prinaša skladnost z zakonodajo o varstvu osebnih podatkov za računovodske servise?
4. Katere so najpogostejše pomanjkljivosti v skladnosti dela računovodskih servisov z zakonodajo s področja varstva osebnih podatkov?
5. Ali so delovni procesi računovodskih servisov v skladu z zakonodajo varstva osebnih podatkov?

Podatki so zbrani z metodo globinskih intervjujev, izvedenih na podlagi strukturiranega vprašalnika. Strukturirana oblika vprašalnika je omogočila primerljivost odgovorov med posameznimi intervjuji, hkrati pa je dopuščala dodatna pojasnila in poglobljene odgovore glede na izkušnje posameznih sogovornikov. Vprašalnik je vsebinsko razdeljen na več tematskih sklopov, ki so sistematično sledili ciljem razprave in raziskovalnim vprašanjem: poznavanje zakonodaje s področja varstva osebnih podatkov, notranja politika v računovodskem servisu, pogodbena ureditev razmerij s strankami, tehnični in organizacijski ukrepi za varstvo osebnih podatkov, skladnost z zakonodajo v praksi in vpliv zakonodaje o varstvu osebnih podatkov na poslovanje računovodskih servisov. Celoten vprašalnik je priložen magistrskemu delu v prilogah.

Vsi podatki, zbrani v okviru empirične raziskave, so obdelani anonimno. Imena in priimki ter nazivi računovodskih servisov niso razkriti, intervjuvanci pa so v magistrskem delu obravnavani zgolj z anonimiziranimi oznakami (INT1–INT8). Anonimizacija vzorca je bila nujna z vidika občutljivosti obravnavane tematike. Namen raziskave je bil pridobiti čim bolj realne in resnične podatke o dejanskem stanju skladnosti z zakonodajo o varstvu osebnih podatkov. Razkritje identitete računovodskih servisov, pri katerih niso izpolnjene vse zakonske zahteve, bi bistveno zmanjšalo pripravljenost za sodelovanje in odkrito razpravo. Poleg tega bi anonimna anketna raziskava zaradi pričakovane neodzivnosti verjetno onemogočila dosego želenega obsega vzorca. Zagotavljanje anonimnosti je tako prispevalo k večji kakovosti podatkov in verodostojnosti ugotovitev raziskave.

V okviru empirične razprave sem izvedla osem globinskih intervjujev z zakonitimi zastopniki manjših računovodskih servisov, ki so hkrati tudi njihovi lastniki. Intervjuji so potekali osebno, bodisi v poslovnih prostorih računovodskih servisov bodisi v kavarnah oziroma lokalih v njihovi neposredni bližini, kar je omogočilo sproščeno, a hkrati profesionalno okolje za razpravo. Osebna izvedba intervjujev je omogočila vzpostavitev zaupanja med raziskovalko in intervjuvanci ter spodbudila bolj odkrito razpravo o obravnavani tematiki. Intervjuji so bili prilagojeni razpoložljivosti sogovornikov, njihova vsebina pa se je dosledno nanašala na vnaprej pripravljena vprašanja. Zbrani kvalitativni podatki so analizirani z uporabo kvalitativne vsebinske analize s tematskim kodiranjem, ki temelji na vnaprej določenih kategorijah. Analiza je izvedena na splošnih teoretičnih načelih, pri čemer tematski sklopi izhajajo iz strukture vprašalnika, raziskovalnih vprašanj in teoretičnih izhodišč magistrskega dela. Postopek analize je potekal v več fazah. V prvi fazi so posamezna vprašanja iz intervjujev razvrščena v tematske sklope (npr. poznavanje zakonodaje, notranja politika, tehnični in organizacijski ukrepi itd.), znotraj katerih so oblikovane kode in podkode. V drugi fazi so odgovori intervjuvancev podrobno analizirani, razvrščeni glede na oblikovane kode in umeščeni v ustrezne kategorije. Rezultati so prikazani v tabelah po sklopih od 1 do 7 v nadaljevanju tega poglavja. Kodirne tabele za analizo intervjujev omogočajo pregled nad razširjenostjo posameznih praks, stališč in zaznanih pomanjkljivosti med intervjuvanci. Takšen način analize omogoča strukturirano, pregledno in sistematično obdelavo podatkov ter identifikacijo najpogostejših vzorcev, praks in izzivov računovodskih servisov pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov. Hkrati omogočajo tudi neposredno povezovanje empiričnih ugotovitev z raziskovalnimi vprašanji in s teoretičnimi izhodišči magistrskega dela.

Empirična raziskava ima določene omejitve, ki jih je treba upoštevati pri interpretaciji rezultatov. Vzorec je relativno majhen in omejen na osem računovodskih servisov, kar pomeni, da ugotovitev ni mogoče neposredno posploševati na celotno populacijo računovodskih servisov v Sloveniji. Poleg tega se raziskava osredotoča na manjše računovodske servise z do devet zaposlenimi, zato rezultati ne odražajo nujno stanja v srednje velikih ali velikih računovodskih servisih. Kljub navedenim omejitvam raziskava

omogoča poglobljen vpogled v konkretne prakse in izzive računovodskih servisov ter predstavlja pomembno izhodišče za nadaljnje raziskave na tem področju.

5.1 Analiza globinskih intervjujev po tematskih sklopih

V tem podpoglavju predstavim analizo osmih globinskih intervjujev, izvedenih v manjših računovodskih servisih. Analiza je razdeljena v sedem tematskih sklopov, in sicer poznavanje zakonodaje, notranja politika v računovodskem servisu, pogodbena ureditev s strankami, tehnični in organizacijski ukrepi, skladnost z zakonodajo v praksi, izzivi ter vpliv zakonodaje. Znotraj posameznih tematskih sklopov obravnavam različna vprašanja iz intervjujev. Odgovore intervjuvancev sem s pomočjo sedmih kodirnih tabel sistematično kodirala in izvedla nadaljnjo analizo.

5.1.1 Poznavanje zakonodaje

V prvem tematskem sklopu sem analizirala odgovore intervjuvancev glede njihovega poznavanja zakonodaje s področja varstva osebnih podatkov in razumevanje ključnih obveznosti, ki jih ta zakonodaja nalaga računovodskim servisom. Analiza temelji na odgovorih, prikazanih v tabeli 1, ki povzema poznavanje zakonodaje računovodskih servisov na področju varstva osebnih podatkov in njihovih ključnih obveznosti.

Tabela 1: Poznavanje zakonodaje

Koda	**Podkoda**	**Oznake intervjujev**
A	**Poznavanje zakonodaje**	
A1	Poznavanje GDPR/ZVOP-2	
	Dobro	INT1–2, INT5, INT8
	Srednje	INT3–4, INT6–7
A2	Ključne obveznosti računovodskih servisov	
	Ureditev dokumentacije in hramba osebnih podatkov	INT1–2, INT7
	Upoštevanje rokov hrambe	INT1–2, INT5–6
	Omejen dostop do podatkov	INT1, INT3–4, INT6. INT8
	Zanesljivi zaposleni	INT6, INT7–8
	Izobraževanje zaposlenih	INT1–3
	Ustrezna varnostna zaščita	INT4, INT6
	Namenska uporaba in preprečevanja razkritij	INT4–5, INT8

Vir: lastno delo.

Intervjuvanci so bili najprej pozvani, da ocenijo svoje poznavanje splošnih zahtev GDPR in ZVOP-2. Odgovori so bili kodirani v okviru kode A1 – Poznavanje GDPR/ZVOP-2, pri čemer sta se med pridobivanjem intervjujev izoblikovali dve podkategoriji – dobro in srednje poznavanje. Rezultati kažejo, da polovica intervjuvancev (INT1, INT2, INT5 in INT8) svoje poznavanje zakonodaje ocenjuje kot dobro, preostali intervjuvanci (INT3, INT4, INT6 in

INT7) pa svoje poznavanje zakonodaje ocenjujejo kot srednje dobro. Nihče izmed sodelujočih svojega poznavanja ni ocenil kot slabo, kar nakazuje, da se računovodski servisi zavedajo pomena varstva osebnih podatkov in osnovnih zakonskih zahtev. Kljub temu je iz odgovorov razvidno, da je pri nekaterih intervjuvancih prisotna določena mera negotovosti glede podrobnejših zakonskih zahtev, kar se odraža v izbiri ocene »srednje«. To lahko kaže na dejstvo, da se zakonodaja sicer pozna na splošni ravni, vendar ne v celoti.

V nadaljevanju so intervjuvanci opisovali, katere ključne obveznosti glede varstva osebnih podatkov po njihovem mnenju zadevajo računovodske servise. Odgovori so bili razvrščeni pod kodo A2 in grafično prikazani v sliki 1. Najpogosteje so intervjuvanci izpostavili pomen omejenega dostopa do osebnih podatkov (INT1, INT3, INT4, INT6 in INT8), pri čemer so poudarili, da naj z osebnimi podatki delajo le pooblaščeni, odgovorni in zaupanja vredni zaposleni (INT6, INT7 in INT8). S tem je tesno povezano tudi izobraževanje zaposlenih, ki so ga kot ključno navedli INT1, INT2 in INT3. Pomemben poudarek je bil tudi na ustrezni hrambi osebnih podatkov (INT1, INT2, INT5 in INT6) in upoštevanju rokov hrambe, kar sta izpostavila predvsem INT 1 in INT5. Več intervjuvancev (INT1, INT2 in INT7) je izpostavilo tudi pomen ureditve ustrezne dokumentacije, kot so pogodbe o obdelavi osebnih podatkov, notranji pravilnik, zbirke osebnih podatkov ipd. Manj pogosto, a še vedno, so intervjuvanci omenili ustrezno varnostno zaščito (INT4 in INT6), uporabo osebnih podatkov izključno za namen, za katerega so bili pridobljeni (INT4), in preprečevanje razkritja osebnih podatkov (INT5 in INT8). To kaže, da se intervjuvanci zavedajo temeljnih načel varstva osebnih podatkov, vendar se poudarki med posamezniki razlikujejo.

Slika 1: Ključne obveznosti računovodskih servisov



Vir: lastno delo.

Analiza odgovorov kaže, da računovodski servisi v splošnem izkazujejo zavedanje pomena zakonodaje s področja varstva osebnih podatkov in osnovnih obveznosti, ki iz nje izhajajo.

Intervjuvanci svoje poznavanje zakonodaje večinoma ocenjujejo kot zadovoljivo, hkrati pa v odgovorih prepoznajo tudi določene omejitve pri razumevanju bolj specifičnih in podrobnih zahtev. Pri opredeljevanju ključnih obveznosti poudarjajo predvsem praktične vidike varstva osebnih podatkov, kot so omejen dostop, ustrezna hramba in izobraževanje zaposlenih, nekoliko manj pa sistematične in formalne vidike, kot so na primer celovita dokumentacija. Skupno ugotovitve kažejo na razmeroma dobro osnovno razumevanje področja varstva osebnih podatkov ob hkratni raznolikosti pristopov in poudarkov v praksi.

5.1.2 Notranja politika v računovodskem servisu

V nadaljevanju sem analizirala odgovore intervjuvancev, ki se nanašajo na notranje ureditve varstva osebnih podatkov v računovodskih servisih. Pri tem sem posebno pozornost namenila vrstam obdelovanih osebnih podatkov, obstoju zbirk osebnih podatkov, imenovanju DPO, internim pravilnikom, usposabljanju zaposlenih in ravnanju v primeru kršitev varstva osebnih podatkov. Analiza temelji na odgovorih, prikazanih v tabeli 2, ki povzema notranjo politiko računovodskih servisov na področju varstva osebnih podatkov.

Tabela 2: Notranja politika v računovodskem servisu

Koda	**Podkoda**	**Oznake intervjujev**
B	**Notranja politika v računovodskem servisu**	
B1	Vrste obdelovanih osebnih podatkov	
	Zaposleni, stranke in pogodbeni sodelavci	INT1–3
	Obračuni plač in pogodbeno delo	INT1–8
	Podatki na pogodbah in računi (fizične osebe)	INT1–5, INT7
	Osebni podatki: ime, priimek, naslov prebivališča, davčna številka	INT1–8
	Osebni podatki: telefonska številka	INT1, INT4, INT6, INT8
	Osebni podatki: EMŠO	INT1–2, INT4–6, INT8
	Osebni podatki: e-poštni naslov	INT1, INT4–8
	Osebni podatki: številka TRR	INT1–4, INT6
B2	Evidentiranje zbirk	
	Zbirke osebnih podatkov: imajo	INT1–2
B2.1	Zbirke osebnih podatkov: nimajo	INT3–8
	Ni sistematičnega pregleda	INT3–8
	Previdno in skrbno ravnanje s podatki (z občutljivimi in osebnimi)	INT4, INT6, INT8
	Sledljivost dostopa in minimizacija podatkov	INT3
B3	Odgovorna oseba za varstvo osebnih podatkov	
	Nimajo	INT1–4, INT6–8
B4	Interni pravilnik	
	Imajo (občasna posodobitev)	INT1–2
	Nimajo	INT3–8

se nadaljuje

Tabela 3: Notranja politika v računovodskem servisu (nad.)

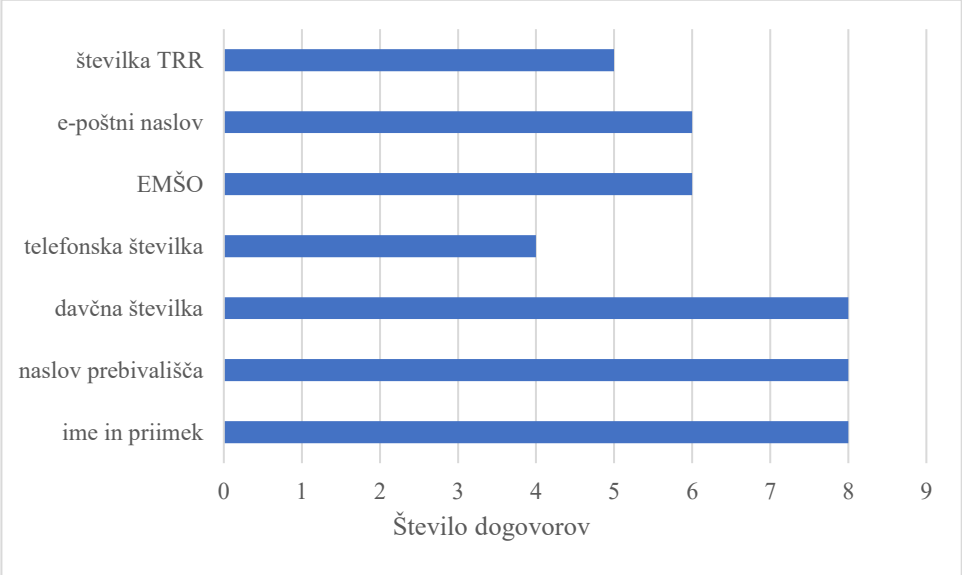
Koda	Podkoda	Oznake intervjujev
B5	Razlogi za neobstoj pravilnika	
	Imajo namen urediti	INT4, INT6, INT7
	Nimajo namena (dvom v doprinos, strošek, nepotrebno)	INT3, INT5, INT8
	Razlog: pomanjkanje časa	INT3–5, INT7
	Razlog: druge prioritete	INT4, INT6
B6	Usposabljanje zaposlenih	
	Dobro/Srednje	INT1–6/ INT7–8
	Usposabljanja: redno, neformalno, znotraj podjetja	INT1–2
	Usposabljanja: samoiniciativno (članki, e-novice), skozi delo	INT3–4, INT7–8
	Brez usposabljanja	INT5–6
B7	Preverjanje znanja	
	Zaupanje (ni sistematičnega preverjanja)	INT1–4, INT6–8
	Ukrepi ob napakah: opozorila	INT1–2, INT5–8
B8	Protokol v primeru kršitve	
	Obstaja (obrazec)	INT1
	Ne obstaja	INT2–8
	Ravnanje: obvestijo stranko (pri večjih napakah)	INT1–8

Vir: lastno delo.

Vsi intervjuvanci so navedli, da v okviru svojega dela obdelujejo širok nabor podatkov, kar je bilo kodirano pod kodo B1 – Vrste obdelovanih osebnih podatkov. Najpogosteje so bili omenjeni podatki, povezani z obračuni plač in drugimi oblikami pogodbenega dela, kar so izpostavili vsi intervjuvanci (INT1–INT8). Prav tako so pogosto navedli podatke o zaposlenih (INT1, INT2 in INT3), podatke o strankah (INT1, INT2 in INT3), podatke o pogodbenih sodelavcih strank (INT2 in INT3), podatke na pogodbah (INT1, INT2, INT3, INT4 in INT5) in računih izdanim fizičnim osebam (INT1, INT2, INT3, INT4 in INT7). Pri konkretnih vrstah osebnih podatkov so rezultati grafično prikazani na sliki 2. Vsi (INT1–INT8) intervjuvanci so soglasno navedli osnovne identifikacijske podatke, kot so ime, priimek, naslov prebivališča in davčna številka. Poleg tega so bili pogosto omenjeni tudi EMŠO (INT1, INT2, INT4, INT5, INT6 in INT8), številka transakcijskega računa (INT1, INT2, INT3, INT4 in INT6), telefonska številka (INT1, INT4, INT6 in INT8) in e-poštni naslov (INT1, INT4, INT5, INT6, INT7 in INT8). Na podlagi navedenega lahko sklepam, da računovodski servisi pri svojem delu obdelujejo razmeroma obsežen nabor osebnih

podatkov, pri čemer se največji del teh podatkov pojavlja v povezavi z obračuni plač in drugimi oblikami pogodbenega dela.

Slika 2: Vrste obdelovanih osebnih podatkov



Vir: lastno delo.

V nadaljevanju so na vprašanje, zajeto pod kodo B2 – Evidentiranje zbirk, intervjuvanci odgovarjali na vprašanje o obstoju zbirk osebnih podatkov, pri čemer sta pritrdilno odgovorila dva intervjuvanca (INT1 in INT2), medtem ko so ostali (INT3–INT8) navedli, da takšnih zbirk nimajo. To lahko pomeni, da se računovodski servisi med seboj razlikujejo v tem, kako jasno in sistematično imajo urejeno evidentiranje in upravljanje osebnih podatkov oziroma kako formalno so ti postopki zapisani in izvajani v praksi.

Intervjuvanci, ki nimajo posebej opredeljenih zbirk osebnih podatkov, so nadalje odgovarjali na vprašanje B2.1. Namen tega vprašanja je bil ugotoviti, kako v takšnih primerih kljub temu ohranjajo pregled nad tem, katere osebne podatke obdelujejo in kako z njimi ravnajo. Intervjuvanci so kot nadomestilo za formalno zbirko navajali predvsem splošno skrbno ravnanje z osebnimi podatki (INT4, INT6, INT8). Nekateri so izpostavili tudi sprotno brisanje osebnih podatkov iz e-pošte (INT3), pazljivost, da se osebni podatki uporabljajo le za namen, za katerega so bili pridobljeni (INT3), omejen dostop do podatkov (INT3) in sledljivost dostopov prek računovodskih programov (INT3). Takšen pristop kaže na bolj neformalno upravljanje obdelave osebnih podatkov. Čeprav intervjuvanci poudarjajo previdnost in odgovoren odnos do varstva osebnih podatkov, lahko pomanjkanje sistematičnega pregleda nad zbirkami pomeni večje tveganje za neskladnost z zakonodajo.

Analiza kode B3 – Odgovorna oseba za varstvo osebnih podatkov je pokazala, da nobeden izmed intervjuvancev (INT1–INT8) nima imenovane pooblaščene osebe za varstvo osebnih podatkov. To kaže, da večina manjših računovodskih servisov področje varstva osebnih podatkov obravnava kot del rednih delovnih nalog in ne kot samostojno funkcijo. Skrb za

osebne podatke je tako razpršena med zaposlene ali prepuščena vodstvu. Ob tem je treba poudariti, da večina manjših podjetij k imenovanju DPO zakonsko res ni zavezana, kar so nekateri intervjuvanci tudi izpostavili.

Vprašanje glede obstoja pravilnikov sem obravnavala v okviru kode B4 – Interni pravilnik. Le dva intervjuvanca (INT1 in INT2) sta navedla, da imata vzpostavljen notranji pravilnik o varstvu osebnih podatkov, ki ga občasno tudi posodabljata. Večina intervjuvancev (INT3–INT8) pa takšnega pravilnika nima. Nadalje so v okviru kode B5 – Razlogi za neobstoj pravilnika intervjuvanci podali več razlogov za to stanje. Med njimi je bil najpogostejši pomanjkanje časa (INT3, INT4, INT5 in INT7). Pogosto so kot odgovor navedli tudi dvom v doprinos k izboljšanji kakovosti njihove storitve (INT3, INT5, INT8), dodaten strošek (INT3, INT5), prioritizacijo drugega dela (INT4, INT6) in celo nepotrebnost (INT8). Kljub temu so nekateri intervjuvanci izrazili namen vzpostaviti notranjo politiko oziroma pravilnik o varstvu osebnih podatkov (INT4, INT6, INT7), medtem ko drugi tega ne načrtujejo (INT3, INT5, INT8). Ti odgovori kažejo na zaznavanje varstva osebnih podatkov predvsem kot neko administrativno breme, ne pa kot orodje, ki bi lahko prispevalo k večji urejenosti, preglednosti in obvladovanju tveganj v njihovem poslovanju.

Usposabljanje zaposlenih je bilo analizirano pod kodo B6 – Usposabljanje zaposlenih. Večina intervjuvancev je ocenila raven znanja zaposlenih kot dobro (INT1, INT2, INT3, INT4, INT5, INT6), nekateri pa kot srednje dobro (INT7, INT8). Kljub temu so načini usposabljanja med računovodskimi servisi precej raznoliki. Redna letna usposabljanja izvajata le dva servisa (INT1 in INT2), medtem ko se drugi zanašajo na neformalne oblike pridobivanja znanja, kot so revije, članki, e-novice (INT3, INT7, INT8), vsakodnevno delo (INT4) ali pa posebnih usposabljanj sploh ne izvajajo (INT5, INT6).

Tudi preverjanje znanja zaposlenih, analizirano pod kodo B7 – Preverjanje znanja, v večini ni sistematično (INT1, INT2, INT3, INT4, INT6, INT7). Intervjuvanci so pri tem poudarili predvsem zaupanje v zaposlene (INT1, INT2, INT8), uporabo spodbud (INT6) in opozarjanje v primeru zaznanih napak (INT1, INT2, INT5, INT6, INT7, INT8). Formalnih oblik preverjanja znanja zaposlenih, kot so testi ali redna ocenjevanja, praviloma ne izvajajo.

Na podlagi navedenega lahko sklepamo, da se računovodski servisi večinoma zanašajo na osebno odgovornost zaposlenih in sprotno učenje v praksi, pri čemer formalno načrtovana usposabljanja in preverjanja znanja niso v ospredju. Takšen pristop lahko v manjših okoljih deluje učinkovito, vendar hkrati pomeni, da je raven znanja bolj odvisna od posameznikov in manj od sistematično urejenih postopkov, kar lahko vpliva na doslednost pri varstvu osebnih podatkov.

Zadnji sklop znotraj teme notranje politike v računovodskem servisu se nanaša na kodo B8 – Protokol v primeru kršitve varstva osebnih podatkov. Le en intervjuvanec (INT1) je navedel, da ima vzpostavljen formaliziran protokol, in sicer v obliki obrazca za obveščanje posameznika o morebitni kršitvi varstva osebnih podatkov. Ostali intervjuvanci (INT2–

INT8) takšnega protokola nimajo. Kljub temu so vsi intervjuvanci poudarili, da bi v primeru kršitve o tem obvestili svoje stranke (INT1–INT8). Pri tem je en intervjuvanec (INT7) izpostavil, da v primeru manjše napake obveščanja ne bi izvedel. Zanimivo je tudi, da nobeden od intervjuvancev ni navedel, da bi v primeru kršitve obvestil Informacijskega pooblaščenca.

Analiza notranjih ureditev varstva osebnih podatkov kaže, da računovodski servisi pri svojem delu obdelujejo obsežen nabor osebnih podatkov, predvsem v povezavi z obračuni plač in s pogodbenimi razmerji, pri čemer se med njimi razlikuje stopnja formalizacije notranjih postopkov. Večina intervjuvancev ne vodi posebej opredeljenih zbirk osebnih podatkov, nima imenovane pooblaščene osebe za varstvo osebnih podatkov in ne razpolaga z vzpostavljenimi notranjimi pravilniki ali s formalnimi protokoli za ravnanje v primeru kršitev. Varstvo osebnih podatkov je večinoma vključeno v vsakodnevno delo in temelji na povečani previdnosti pri obdelavi osebnih podatkov, osebni odgovornosti zaposlenih ter neformalnih oblikah usposabljanja in preverjanja znanja. Takšen pristop omogoča prilagodljivost v manjših delovnih okoljih, hkrati pa vodi v raznolike prakse in manj sistematičen pregled nad obdelavo osebnih podatkov med posameznimi računovodskimi servisi.

5.1.3 Pogodbena ureditev s strankami

V tem tematskem sklopu sem analizirala odgovore intervjuvancev, prikazanih v tabeli 3, ki prikazuje ureditev pogodbenih razmerij s strankami, ki v tem odnosu nastopajo v vlogi upravljavca osebnih podatkov. Osredotočila sem se tudi na vodenje evidenc obdelave ter določanje in nadzor rokov hrambe osebnih podatkov. Sklop se neposredno nanaša na vprašanja, kako so zahteve zakonodaje s področja varstva osebnih podatkov prenesene v prakso računovodskih servisov.

Tabela 4: Pogodbena ureditev s strankami

Koda	**Podkoda**	**Oznake intervjujev**
C	**Pogodbena ureditev s strankami**	
C1	Pogodbe o obdelavi	
	Imajo (z vsemi/z nekaterimi)	INT1/INT2
	Nimajo	INT3–8
	Razlogi: pomanjkanje časa	INT3–4, INT6–7
	Razlogi: jim ni prioriteta	INT7–8
	Razlogi: dodaten strošek in delo	INT3, INT5
C2	Evidence dejavnosti obdelave	
	Ne vodijo	INT1–8
C3	Roki hrambe	
	Določeni v zbirkah OP (široko zastavljeni)	INT1–2
	Niso formalno določeni	INT1, INT4

se nadaljuje

Tabela 5: Pogodbena ureditev s strankami (nad.)

Koda	Podkoda	Oznake intervjujev
	Vezano na poslovno razmerje/računovodske predpise	INT1–2, INT4 / INT6–7
	Brisanje: ob prenehanju sodelovanja/sprotno	INT1, INT4, INT6/INT3
	Trajna hramba: plače (zakonska zahteva)	INT1–2, INT4–6, INT8
	Vračanje fizične dokumentacije stranki	INT2, INT4–8
	Upoštevanje rokov v računovodstvu/trajna hramba	INT5, INT7/INT3, INT5–8
	Neurejeno področje/prepustijo stranki	INT4–6, INT7

Vir: lastno delo.

Vprašanje o sklenjenih pogodbah o obdelavi osebnih podatkov s strankami sem obravnavala v okviru kode C1 – Pogodbe o obdelavi. Rezultati intervjujev kažejo, da ima pogodbe o obdelavi osebnih podatkov z vsemi strankami sklenjene le en intervjuvanec (INT1), medtem ko ima en intervjuvanec takšne pogodbe sklenjene le z delom svojih strank (INT2). Večina intervjuvancev (INT3–INT8) pogodb o obdelavi osebnih podatkov nima. Kot najpogostejši razlog za neobstoj pogodb so intervjuvanci navedli pomanjkanje časa (INT3, INT4, INT6, INT7), dodatne stroške in delo (INT3 in INT5) in dejstvo, da pogodbenih ureditev ne smatrajo kot prioriteto (INT7, INT8). Na podlagi odgovorov lahko sklepamo, da je področje pogodbenega urejanja obdelave osebnih podatkov v računovodskih servisih pogosto zapostavljeno, čeprav gre za pomemben element jasne razmejitve med ponudnikom storitev in stranko. Odsotnost tovrstnih pogodb lahko v praksi vodi v nejasnosti glede obveznosti posameznih strani, zlasti v primeru neskladnosti ali morebitnih kršitev varstva osebnih podatkov.

V okviru kode C2 – Evidenca dejavnosti obdelave so intervjuvanci odgovarjali na vprašanja glede evidenc dejavnosti obdelave osebnih podatkov. Analiza odgovorov je pokazala, da nobeden izmed intervjuvancev (INT1–INT8) ne vodi takšnih evidenc. Glede na velikost intervjuvanih računovodskih servisov in naravo njihovega dela to načeloma zanje ni zakonska obveznost. Po določbah GDPR namreč evidence dejavnosti obdelave praviloma niso obvezne za organizacije z manj kot 250 zaposlenimi, razen v primerih, ko obdelava osebnih podatkov ni zgolj občasna, vključuje posebne vrste osebnih podatkov ali predstavlja večje tveganje za pravice in svoboščine posameznikov (30. člen GDPR). V takšnih primerih bi morale evidenco dejavnosti obdelave voditi tudi manjše družbe, kot so intervjuvani računovodski servisi. Na podlagi navedenega lahko sklepamo, da odsotnost evidenc dejavnosti obdelave pri intervjuvancih ni nujno odraz neupoštevanja zakonodaje, temveč predvsem odraz njihove velikosti in razumevanja zakonodaje. Kljub temu bi lahko vodenje tovrstnih evidenc, tudi kadar niso izrecno obvezne, prispevalo k boljšemu pregledu nad obdelavo osebnih podatkov in večji preglednosti notranjih procesov.

Vprašanja, povezana z roki hrambe osebnih podatkov, sem analizirala v okviru kode C3 – Roki hrambe. Le dva intervjuvanca (INT1 in INT2) sta navedla, da imajo roke hrambe jasno določene v zbirkah osebnih podatkov, medtem ko pri večini intervjuvancev (INT3–INT8) ti

roki niso formalno opredeljeni. Na vprašanje, kako v praksi določajo in nadzorujejo roke hrambe osebnih podatkov, so intervjuvanci navajali različne pristope. Najpogosteje so omenjali trajno hrambo določenih zbirk, ki je zakonsko obvezna, kot so na primer podatki, povezani z obračuni plač (INT1, INT2, INT4, INT5, INT6, INT8), in vračanje poslovne dokumentacije strankam v fizični obliki (INT2, INT4, INT5, INT6, INT7, INT8). Nekateri so pojasnili, da roke hrambe vežejo na poslovno razmerje s strankami (INT1, INT2, INT4) in da osebne podatke ob prenehanju sodelovanja s stranko izbrišejo (INT1, INT4, INT6). Poleg tega so nekateri intervjuvanci navedli, da si delo olajšajo s široko zastavljenimi roki hrambe (INT1, INT2) in z upoštevanjem rokov, določenih v računovodskih predpisih (INT6, INT7). Posamezni intervjuvanec (INT3) je izpostavil tudi nekoliko drugačen pristop, in sicer sprotno brisanje osebnih podatkov, izogibanje njihovemu shranjevanju in uporabo računovodskega programa, ki je dostopen prek brskalnika, kjer ima računovodstvo zgolj dostop, podatki pa ostajajo pri upravljavcu. Nekateri intervjuvanci so priznali, da nimajo sistematičnega nadzora nad upoštevanjem rokov hrambe (INT1, INT4).

Na podlagi navedenega lahko sklepamo, da se roki hrambe osebnih podatkov v računovodskih servisih pogosto urejajo bolj na podlagi ustaljene prakse in zakonskih zahtev s področja računovodstva kot pa z jasno določenimi pravili varstva osebnih podatkov. Takšen pristop lahko v vsakodnevnem delu deluje praktično, vendar hkrati pomeni manjši pregled nad tem, kateri osebni podatki se hranijo in kako dolgo, kar lahko predstavlja izziv z vidika skladnosti in preglednosti.

Na splošno lahko sklepamo, da je področje pogodbenega urejanja in upravljanja obdelave osebnih podatkov v računovodskih servisih urejeno precej neenotno, pogosto bolj neformalno. Pogodbe o obdelavi, evidence dejavnosti obdelave in jasno določeni roki hrambe pogosto niso vzpostavljeni, kar je deloma povezano z velikostjo servisov in deloma z razumevanjem zakonodaje in s praktičnimi omejitvami v vsakodnevnem delu. Računovodski servisi se pri ravnanju z osebnimi podatki pogosto opirajo na ustaljene prakse in zahteve računovodske zakonodaje, medtem ko so vidiki varstva osebnih podatkov manj sistematično vključeni v njihove procese. Takšen pristop sicer omogoča nemoteno izvajanje dela, vendar lahko vodi v manjšo preglednost, nejasnosti glede odgovornosti in večje tveganje v primeru sporov ali kršitev.

5.1.4 Tehnični in organizacijski ukrepi

V tem tematskem sklopu sem analizirala odgovore intervjuvancev glede tehničnih in organizacijskih ukrepov, ki jih uporabljajo za zagotavljanje varnosti osebnih podatkov, nadzora dostopa in IT-varnosti. Odgovori intervjuvancev so strnjeni v tabeli 4, ki prikazuje, katere tehnične in organizacijske ukrepe za varstvo osebnih podatkov uporabljajo intervjuvanci.

Tabela 6: Tehnični in organizacijski ukrepi

Koda	Podkoda	Oznake intervjujev
D	**Tehnični in organizacijski ukrepi**	
D1	Varni prenos, hramba	
	Ukrepi za varstvo vseh podatkov (ne le OP)	INT1, INT4–7
	Dokumentacija in pravilniki	INT1
	Nadzor dostopa	INT1–8
	IT-varnostne prakse	INT1–8
D2	Nadzor dostopa	
	Zaklepanje prostorov in omar	INT1–8
	Tehnično varovanje (alarm, kamere)	INT1, INT4–6
	Kontrola pristopa (videofon, kartice)	INT1, INT4, INT6–7
	Kontrola pristopa: zaupanje zaposlenim	INT2, INT6–8
	Gesla za računalnik in programe	INT1–8
D3	IT-varnostne prakse	
	Gesla za računalnik in programe	INT1–8
	Dvofaktorska avtentikacija	INT1, INT5–6
	Antivirusna zaščita in varnostne kopije	INT1, INT6–7
	Šifriranje e-pošte	INT1–4, INT6–8
	Varnostne kopije	INT1–2, INT4–8
D4	Dostopnost varnostnih kopij	
	Dostop: Zastopnik/stranka	INT1–6, INT8 / INT3
	Dostop: IT-osebje	INT1, INT3–4, INT6–8
	Hramba: v prostorih podjetja	INT1, INT4–8
	Hramba: na drugi lokaciji/V oblaku	INT1–2/INT3, INT6

Vir: lastno delo.

Odgovore na vprašanje glede uvedenih ukrepov za varen prenos, hrambo in dostop do osebnih podatkov sem analizirala pod kodo D1 – Varen prenos in hramba. Intervjuvanci so opisovali različne fizične in organizacijske ukrepe, pri čemer so poudarili, da večina teh ukrepov ni bila uvedena izključno zaradi varstva osebnih podatkov, temveč zaradi varstva vseh občutljivih podatkov, ki se obdelujejo v računovodstvu (INT1, INT4, INT5, INT6, INT7). Le en intervjuvanec (INT1) je kot ukrep izpostavil sprejetje predpisane dokumentacije in pravilnikov s področja varstva osebnih podatkov. Vsi intervjuvanci (INT1–INT8) pa so navedli, da izvajajo določeno obliko nadzora dostopa in uporabo IT-varnostnih praks, ki se med intervjuvanci razlikujejo. Ti ukrepi kažejo, da računovodski servisi izvajajo predvsem varnostne prakse, ki so pogosto že del splošnega poslovnega delovanja in niso nujno posebej prilagojene zahtevam zakonodaje s področja varstva osebnih podatkov. Čeprav ti ukrepi pomembno prispevajo k zaščiti osebnih podatkov, so le redko načrtovani in prilagojeni izključno z vidika zahtev zakonodaje, kar kaže na bolj splošen in manj sistematičen pristop k temu področju.

Odgovore na vprašanje o tem, kako je zagotovljeno, da do osebnih podatkov dostopajo le pooblaščene osebe, sem analizirala v okviru kode D2 – Nadzor dostopa. Intervjuvanci so

najpogosteje navajali uporabo gesel za dostop do računalnikov (INT1, INT2, INT3, INT4, INT5, INT6, INT7 in INT8) in računovodskih programov (INT1, INT2, INT3, INT4, INT5, INT6). Poleg teh ukrepov so izpostavili tudi fizično omejevanje dostopa, kot so zaklepanje poslovnih prostorov (INT1–8), zaklepanje omar, odpiranje preko videofona/zvonca (INT1, INT4, INT6–7). Nekateri intervjuvanci dostop omejujejo tudi z alarmnimi napravami (INT1, INT4–6) in s sledljivostjo vstopa zaposlenih v poslovne prostore s pomočjo kode ali kartice (INT6). Ob tem so posamezni intervjuvanci posebej izpostavili tudi pomen zaupanja vrednih zaposlenih (INT2, INT6–8). Na podlagi odgovorov lahko sklepamo, da računovodski servisi nadzor dostopa do osebnih podatkov zagotavljajo predvsem s kombinacijo tehničnih in organizacijskih ukrepov, pri čemer ima pomembno vlogo tudi zaupanje v zaposlene. Takšen pristop je v manjših delovnih okoljih razumljiv in pogosto učinkovit, vendar je hkrati močno odvisen od odgovornosti posameznikov, manj pa od formalno določenih in dosledno nadzorovanih postopkov.

V okviru kode D3 – IT-varnostne prakse so intervjuvanci opisovali, katere tehnične rešitve uporabljajo za zaščito osebnih podatkov. Večina jih je navedla, da pri pošiljanju dokumentov po e-pošti, predvsem v zvezi s plačami in z drugimi oblikami pogodbenega dela, uporabljajo šifriranje (INT1, INT2, INT3, INT4, INT6, INT7, INT8), prav tako redno izvajajo varnostne kopije podatkov (INT1, INT2, INT4, INT5, INT6, INT7, INT8). Nekaj intervjuvancev je omenilo tudi uporabo dvofaktorske prijave (INT1, INT5, INT6) in antivirusnih programov (INT1, INT7). V okviru kode D4 – Dostopnost varnostnih kopij sem preverjala, kje se varnostne kopije hranijo in kdo ima do njih odstop. Po besedah intervjuvancev se varnostne kopije hranijo na različnih lokacijah, najpogosteje v poslovnih prostorih podjetja (INT1, INT4, INT5, INT6, INT7, INT8), občasno tudi na drugi lokaciji (INT1, INT2) ali kar v oblaku (INT3, INT6). Dostop do teh kopij imajo intervjuvanci (INT1, INT2, INT3, INT4, INT5, INT6, INT8) kot zastopniki računovodskih servisov in IT-osebje (INT1, INT3, INT4, INT6, INT7, INT8) ter v primeru enega intervjuvanca (INT3) tudi stranke. V nobenem primeru dostopa do teh kopij nimajo zaposleni ali katere koli zunanje osebe. Na podlagi navedenega lahko sklepamo, da računovodski servisi razmeroma dosledno uporabljajo IT-varnostne ukrepe, zlasti na področju varnostnega kopiranja in zaščite podatkov, do katerih ima dostop majhen krog ljudi. Ob tem pa je treba ponovno poudariti, da ti ukrepi najverjetneje niso bili uvedeni izključno za varstvo osebnih podatkov, temveč so namenjeni širšemu varovanju vseh občutljivih podatkov, s katerimi računovodski servisi razpolagajo v okviru svojega poslovanja.

Na splošno lahko ugotovim, da računovodski servisi na področju tehničnih in organizacijskih ukrepov izvajajo predvsem osnovne in razmeroma dobro uveljavljene varnostne prakse. Ti ukrepi so večinoma del splošnega poslovnega delovanja in so namenjeni zaščiti vseh občutljivih podatkov, ne zgolj osebnih. Varnostni mehanizmi za prenos, hrambo in dostop do podatkov ter IT-varnostne rešitve, kot so varnostne kopije in omejen dostop, so praviloma prisotni, vendar pogosto niso načrtovani izključno z vidika varovanja osebnih podatkov. Nadzor dostopa temelji predvsem na zaupanju v zaposlene in

manjših, bolj preglednih delovnih okoljih, kar pomeni manj sistematičen pristop. Sklepno lahko ocenim, da so temelji varovanja osebnih podatkov v računovodskih servisih postavljeni, vendar obstaja prostor za bolj premišljeno in ciljno usmerjeno prilagoditev ukrepov z vidika zakonodaje o varstvu osebnih podatkov.

5.1.5 Skladnost z zakonodajo v praksi

Ta tematski sklop se nanaša na samooceno skladnosti, izkušnje z nadzori in ravnanje ob uveljavitvi pravic posameznikov. Analiza temelji na odgovorih intervjuvancev, ki so sistematično zbrani in prikazani v tabeli 5, ki ponuja pregled skladnosti dela računovodskih servisov z zakonodajo v praksi.

Tabela 7: Skladnost z zakonodajo v praksi

Koda	**Podkoda**	**Oznake intervjujev**
E	**Skladnost z zakonodajo v praksi**	
E1	Ocena skladnosti	
	Visoka	INT1–2
	Srednja	INT3–8
	Manjka dokumentacija, pogodbe, roki hrambe	INT3–8
	Izobraževanje zaposlenih	INT6–7
E2	Revizije/Nadzori	
	Niso imeli	INT1–8
E3	Obravnava pravic posameznikov	
	Zahtev ni	INT1–3, INT5
	Posredovanje zahtev stranki (upravljavcu)	INT1–2, INT4, INT8
	Izpolnitev zahteve posameznika	INT5–8
	Komunikacija izključno s stranko	INT1–2, INT4, INT8
E4	Ravnanje pri zahtevkih posameznikov	
	Posredovanje zahteve stranki (upravljavcu)/pridobitev dovoljenja	INT1–5
	Komunikacija izključno s stranko – zahtevam ne ugodijo	INT1, INT3–4, INT8
	Omejitev izbrisa (zakonska hramba)	INT1, INT3, INT5–7
E5	Postopek v primeru zahteve	
	Nimajo	INT3, INT6–7
	Neformalni: Posredovanje podatkov stranki (upravljavcu)	INT1–2, INT4, INT5, INT8
	Neformalni: Posvet zaposlenih z odgovorno osebo	INT1, INT2, INT8

Vir: lastno delo.

Odgovore o samooceni skladnosti z zakonodajo s področja varstva osebnih podatkov sem analizirala v okviru kode E1 – Ocena skladnosti. Dva intervjuvanca (INT1, INT2) sta skladnost svojega računovodskega servisa ocenila kot visoko, medtem ko večina intervjuvancev (INT3, INT4, INT5, INT6, INT7, INT8) meni, da je njihova skladnost srednje dobra. Kot manj urejena področja so intervjuvanci najpogosteje izpostavili neurejeno

dokumentacijo (INT3, INT4, INT5, INT6, INT7, INT8), dejstvo, da nimajo sklenjenih pogodb o obdelavi osebnih podatkov s čisto vsemi strankami (INT2), nejasno določene roke hrambe (INT6, INT7, INT8) in pomanjkanje izobraževanja zaposlenih (INT6, INT7). Posamezni intervjuvanec (INT1) je izpostavil tudi to, da dokumentacije ne posodabljajo vsako leto, ampak le občasno, ob kakšnih večjih spremembah. Nihče od intervjuvancev (INT1–INT8) še ni imel izkušnje z notranjo ali zunanjo revizijo oziroma nadzorom s področja varstva osebnih podatkov, kar sem analizirala v sklopu kode E2 – Revizije/Nadzori. Na podlagi navedenega lahko sklepamo, da se računovodski servisi svoje skladnosti z zakonodajo sicer zavedajo in jo ocenjujejo kot zadovoljivo, hkrati pa prepoznavajo tudi konkretna področja, kjer vidijo največ izzivov in neskladnosti. Odsotnost revizij in nadzorov lahko pomeni manjši zunanji pritisk na izboljšave, kar posledično vodi v počasnejše in bolj postopno urejanje področja varstva osebnih podatkov.

Vprašanja, povezana z obravnavo pravic posameznikov, so bila analizirana pod kodo E3 – Obravnava pravic posameznikov. Intervjuvanci so opisovali tako svoje dosedanje izkušnje kot tudi na splošno prakso ravnanja v primerih, ko bi posamezniki želeli uveljavljati svoje pravice, kot so dostop, popravek ali izbris osebnih podatkov. Več intervjuvancev (INT1, INT2, INT3, INT5) je navedlo, da do sedaj še niso prejeli nobenih zahtev posameznikov za uveljavitev pravic. Iz odgovorov je razvidno, da v praksi računovodski servisi ne komunicirajo neposredno s posamezniki, temveč poteka komunikacija izključno preko strank, ki v razmerju nastopajo kot upravljavci osebnih podatkov, kar so nekateri intervjuvanci (INT1, INT2, INT4, INT8) tudi izpostavili. Intervjuvanci so poudarili, da posamezniki svoje pravice praviloma uveljavljajo pri naročnikih, računovodski servis pa pri tem nastopa kot obdelovalec osebnih podatkov. Kljub temu so nekateri intervjuvanci (INT5, INT6, INT7, INT8) navedli, da bi v primeru prejema zahteve posameznika zahtevo izpolnili, pri čemer so drugi (INT2, INT6) poudarili, da obdelavo osebnih podatkov izvajajo na podlagi zakonskih zahtev. Eden izmed intervjuvancev (INT1) je navedel tudi, da so strankam ob podpisu pogodb o obdelavi osebnih podatkov dali tudi obvestilo o varstvu in obdelavi osebnih podatkov, na katerem jasno pišejo vse njihove pravice. Iz odgovorov je razvidno, da je obravnava pravic posameznikov večinoma posredna in pogojena z vlogo naročnika, torej stranke. Pri tem računovodski servisi nimajo veliko lastnih izkušenj z neposrednim reševanjem takšnih zahtev.

Odgovori na vprašanje, kako bi intervjuvanci ravnali v primeru, če bi posameznik neposredno zahteval uveljavitev svojih pravic do dostopa, popravka ali izbrisa osebnih podatkov, so bili analizirani pod kodo E4 – Ravnanje pri zahtevkih posameznikov. Čeprav je eden izmed intervjuvancev (INT1) izpostavil, da tovrstnega primera v njihovem računovodskem servisu še niso imeli, je več intervjuvancev (INT1, INT3, INT4, INT8) poudarila, da zahtevam posameznikov načeloma ne morejo ugoditi neposredno, saj z njimi nimajo neposrednega stika oziroma za to nimajo pooblastil. Najpogostejša praksa (INT1, INT2, INT3, INT4, INT5) je, da se zahteve posameznikov posredujejo stranki oziroma delodajalcu, ki nastopa kot upravljavec osebnih podatkov ali pa se pred obravnavo zahteve

pridobi dovoljenje stranke. Intervjuvanci (INT1, INT3, INT5, INT7) so večkrat izpostavili tudi, da je pravica do izbrisa osebnih podatkov omejena zaradi zakonsko določenih obveznosti hrambe, zlasti na področju obračuna plač in davčne zakonodaje. Nekateri intervjuvanci (INT6, INT7) so navedli, da zahtevam posameznikov lahko ugodijo v okviru zakonskih možnosti, vendar ob upoštevanju veljavnih predpisov. Iz odgovorov je razvidno, da je ravnanje ob zahtevkih posameznikov v praksi situacijsko, brez vnaprej določenih enotnih postopkov, pri čemer ključno vlogo igra sodelovanje s stranko kot upravljavcem osebnih podatkov.

Odgovori na vprašanja o obstoju posebnih postopkov za primer, ko posameznik neposredno naslovi zahtevo na računovodski servis, so bili analizirani pod kodo E5 – Postopek v primeru zahteve. Več intervjuvancev (INT3, INT6, INT7) je navedlo, da nimajo določenih formalnih postopkov za takšne primere. Namesto formaliziranih postopkov se v praksi uporabljajo neformalni dogovori in splošna pravila ravnanja zaposlenih. Nekateri intervjuvanci (INT1, INT4) so poudarili, da zaposleni ne smejo razkrivati nobenih podatkov neposredno posameznikom, temveč morajo posameznika napotiti nazaj k delodajalcu oziroma naročniku (INT4, INT8). V primeru prejema zahteve posameznika intervjuvanci (INT1, INT2, INT4, INT5) pogosto najprej kontaktirajo stranko in preverijo zahtevo, preden se sprejme kakršna koli odločitev. Prav tako so navedli (INT1, INT2, INT8), da se morajo zaposleni v primeru nejasnosti posvetovati z odgovorno osebo ali nadrejenim. Iz odgovorov je razvidno, da postopki za obravnavo neposrednih zahtev posameznikov večinoma niso formalno opredeljeni, temveč temeljijo na splošnih navodilih, previdnosti zaposlenih in sprotnem usklajevanju s strankami.

Analiza vprašanj E1–E5 kaže, da se računovodski servisi svoje skladnosti z zakonodajo zavedajo in jo ocenjujejo kot splošno dobro. Hkrati prepoznavajo tudi konkretna področja neskladnosti, kjer bi bile možne izboljšave. Računovodski servisi v praksi redko obravnavajo zahteve posameznikov neposredno. Ravnanje ob takšnih zahtevah je večinoma neformalno, odvisno od konkretne situacije in vloge naročnika kot upravljavca osebnih podatkov, pri čemer formalni postopki večinoma niso vzpostavljeni.

5.1.6 Izzivi

V tem tematskem sklopu sem analizirala izzive računovodskih servisov pri zagotavljanju skladnosti z zakonodajo s področja varstva osebnih podatkov. Analiza zajema organizacijske, kadrovske in vsebinske izzive ter vprašanja dokumentacije in upravljanja tveganj. Odgovori intervjuvancev so zbrani in prikazani v tabeli 6, ki povzema glavne izzive računovodskih servisov, oceno ustreznosti dokumentacije in tveganja na področju varstva osebnih podatkov.

Tabela 8: Izzivi

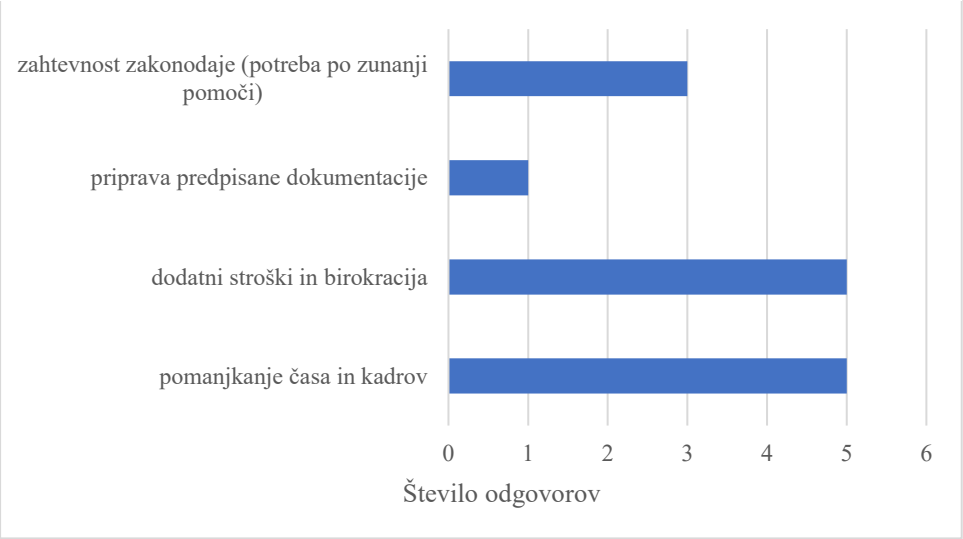
Koda	Podkoda	Oznake intervjujev
F	**Izzivi**	
F1	Glavni izzivi	
	Pomanjkanje časa in kadrov	INT1, INT3–5, INT7
	Dodatni stroški in birokracija	INT1–5
	Priprava predpisane dokumentacije	INT6
	Zahtevnost zakonodaje (potreba po zunanji pomoči)	INT2, INT5, INT8
F2	Dokumentacija	
	Ustrezna	INT1–2
	Ni ustrezna (manjka celotna dokumentacija)	INT3–8
F3	Ocena tveganj	
	Imajo	INT1–2
	Nimajo	INT3–8
F4	Največja tveganja	
	Nizko tveganje	INT2–4, INT6, INT8
	Človeška napaka	INT3–8
	Nepooblaščen dostop, zloraba	INT2–4
	Fizični in IT-vdori, višja sila	INT4–6
	Predolga hramba, hramba napačnih podatkov	INT2–3

Vir: lastno delo.

Vprašanje o glavnih izzivih je bilo analizirano pod kodo F1 – Glavni izzivi. Odgovore intervjuvancev na vprašanje grafično ponazarja slika 3. Večina intervjuvancev (INT1, INT3, INT4, INT5, INT7) je kot največji izziv izpostavila pomanjkanje časa in dodatne stroške (INT1, INT3, INT4, INT5), ki jih prinaša uskladitev z zakonodajo. Varstvo osebnih podatkov pogosto dojemajo kot dodatno delo (INT2, INT4), ki ga morajo opravljati ob že obstoječih računovodskih obveznostih. Poleg časovne obremenitve so intervjuvanci izpostavili tudi dodatno administrativno delo in birokracijo (INT2), ki spremljata zahteve zakonodaje. Nekateri so opozorili na pomanjkanje kadrov (INT1), kar še dodatno otežuje bolj sistematično urejanje tega področja. Dva intervjuvanca (INT2, INT5) sta kot pomemben izziv navedla tudi zahtevnost zakonodaje in pomanjkanje specifičnega znanja, zaradi česar se pojavlja potreba po zunanji, pravni pomoči. Intervjuvanec (INT8) je izpostavil težave pri sledenju pogostim spremembam zakonodaje. Intervjuvanec (INT1) je opozoril tudi na

neodzivnost strank, zlasti pri podpisovanju pogodb o obdelavi osebnih podatkov. Kot izziv je bila izpostavljena tudi na splošno priprava predpisane dokumentacije (INT6).

Slika 3: Glavni izzivi



Vir: lastno delo.

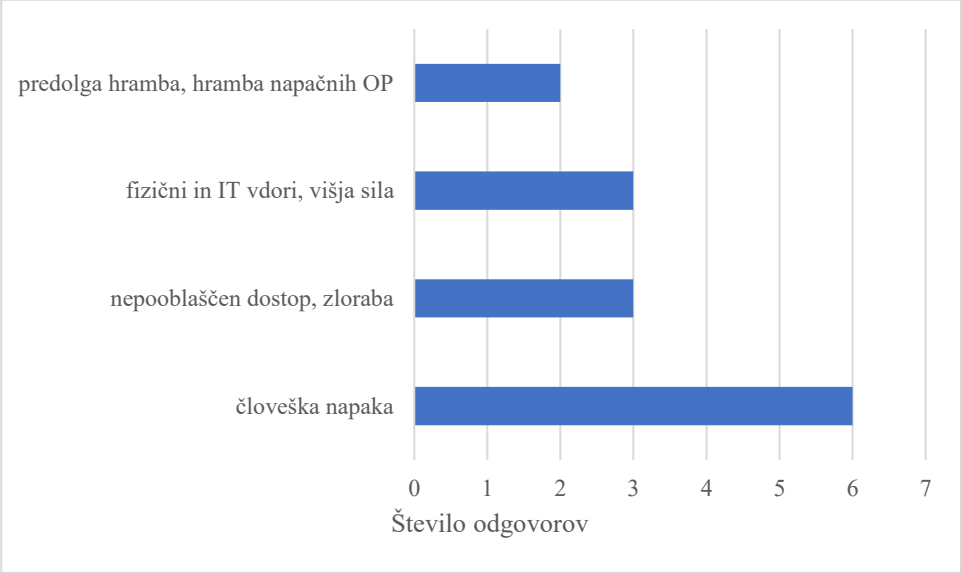
Na podlagi navedenega lahko sklepamo, da računovodski servisi področje varstva osebnih podatkov pogosto doživljajo kot zahtevno in obremenjujoče, predvsem zaradi omejenih virov, zapletenih zahtev, pomanjkanja časa in dodatnih stroškov.

Vprašanja, povezana z ustreznostjo dokumentacije, sem analizirala v sklopu kode F2 – Dokumentacija. Le dva intervjuvanca (INT1, INT2) sta ocenila, da imata dokumentacijo s področja varstva osebnih podatkov urejeno in usklajeno z zakonskimi zahtevami. Večina intervjuvancev (INT3, INT4, INT5, INT6, INT7, INT8) je odkrito navedla, da dokumentacije nimajo oziroma da zato ni skladna z zakonodajo. Kot najpogostejše manjkajoče elemente so intervjuvanci (INT3, INT4, INT5, INT6, INT7, INT8) izpostavili celovito dokumentacijo o obdelavi osebnih podatkov, ki bi jasno opredelila postopke, odgovornosti in pravila ravnanja. V enem primeru (INT2) je bil izpostavljen tudi manjkajoč nabor pogodb o obdelavi osebnih podatkov, saj so te sklenjene le z delom strank. Na podlagi odgovorov lahko sklepamo, da je dokumentacija eno izmed šibkejših področij varstva osebnih podatkov v računovodskih servisih. Čeprav se intervjuvanci pogosto zavedajo njenega pomena, pomanjkanje časa, znanja ali prioritet pomeni, da dokumentacija v praksi pogosto ni vzpostavljena, kar lahko oteži dokazovanje skladnosti z zakonodajo in poveča tveganje ob morebitnih nadzorih.

Vprašanje, povezano z obstojem ocene tveganja, sem analizirala v okviru kode F3 – Ocena tveganj. Odgovori intervjuvancev so grafično prikazani na sliki 4. Le dva intervjuvanca (INT1 in INT2) sta navedla, da imata izdelano oceno tveganj za zlorabo osebnih podatkov, medtem ko večina intervjuvancev (INT3, INT4, INT5, INT6, INT7, INT8) takšne ocene nima. To kaže, da se večina računovodskih servisov tveganj loteva bolj sproti in brez nekega

formalnega pregleda. Odgovore na vprašanje o zaznanih tveganjih sem analizirala pod kodo F4 – Največja tveganja. Večina intervjuvancev (INT2, INT3, INT4, INT6, INT8) je splošno raven tveganja ocenila kot nizko, vendar so hkrati izpostavili več konkretnih tveganj, s katerimi se lahko soočajo v praksi. Najpogosteje so omenjali tveganje človeških napak (INT3, INT4, INT5, INT6, INT7, INT8), zlasti pošiljanja podatkov napačnemu naslovniku. Poleg tega so intervjuvanci izpostavili še tveganje nepooblaščenega dostopa do podatkov (INT2, INT3, INT4), morebitne zlorabe (INT2), vdore v informacijske sisteme (INT4), vlome v poslovne prostore (INT4, INT5, INT6) in izgubo ali uničenje podatkov zaradi nepredvidljivih dogodkov (INT4, INT5). Nekateri intervjuvanci (INT2, INT3) so opozorili tudi na tveganje predolge hrambe osebnih podatkov in obdelave napačnih oziroma neažurnih podatkov (INT2, INT3). Analiza odgovorov kaže, da intervjuvanci prepoznavajo razmeroma širok nabor možnih tveganj, vendar ta tveganja večinoma niso sistematično ocenjena, dokumentirana ali redno spremljana. To pomeni, da se z njimi pogosto soočajo spontano in sproti, brez vnaprej določenih postopkov.

Slika 4: Največja tveganja



Vir: lastno delo.

Analiza sklopa vprašanj F kaže, da se računovodski servisi soočajo predvsem z organizacijskimi in s časovnimi izzivi ter pomanjkanjem bolj strukturiranega pristopa k dokumentaciji in upravljanju tveganj. Čeprav zavedanje o obstoju tveganj nedvomno obstaja, njihovo obvladovanje v praksi večinoma ostaja neformalno, kar lahko v zahtevnejših ali nepredvidenih situacijah predstavlja izziv.

5.1.7 Vpliv zakonodaje

Zadnji sklop analize obravnava vpliv zakonodaje na organizacijo dela in delovne procese v računovodskih servisih. Analiza temelji na odgovorih, zbranih v tabeli 7, ki prikazuje vpliv

zakonodaje na delovne procese ter uvedbo novih storitev in postopkov v računovodskih servisih.

Tabela 9: Vpliv zakonodaje

Koda	Podkoda	Oznake intervjujev
G	**Vpliv zakonodaje**	
G1	Vpliv na delovne procese	
	Povečana previdnost pri obdelavi	INT1–3
	Brez bistvenega vpliva	INT2–8
	Povečana birokracija in potreba po izobraževanju	INT1–3
G2	Nove storitve/postopki	
	Ukrepi za varstvo vseh podatkov (ne le OP)	INT1, INT6
	Ni novih tehnologij/postopkov	INT3–5, INT7–8
	Uvajanje IT-rešitev, dokumentacije in pogodb	INT1–2

Vir: lastno delo.

Odgovore na vprašanje o vplivu zakonodaje na delovne procese sem obravnavala v okviru kode G1 – Vpliv na delovne procese. Intervjuvanci so najpogosteje navedli, da je zakonodaja prinesla večjo previdnost pri ravnanju in razkrivanju osebnih podatkov (INT1, INT2 in INT3). Kljub temu je večina intervjuvancev (INT2, INT3, INT4, INT5, INT6, INT7, INT8) poudarila, da zakonodaja ni bistveno spremenila osnovnega procesa računovodskega dela. Kot glavni vpliv so nekateri navedli predvsem povečano količino administrativnih nalog (INT2), potrebo po dodatnem izobraževanju zaposlenih (INT1), dodatno področje, na katerem se je treba izobraževati (INT3), ter večjo porabo časa (INT2), ki je namenjena spremljanju zakonodaje in urejanju dokumentacije. Odgovori tako kažejo, da uvedba zakonodaje ni imela večjega vpliva na vsakodnevne delovne procese v računovodstvu. To bi morda lahko deloma pripisali tudi dejstvu, da večina intervjuvanih še nima v celoti urejene predpisane dokumentacije. Nekateri so omenjali vpliv zakonodaje bolj na podporne in administrativne dejavnosti, ne pa na samo jedro računovodske storitve.

Vprašanja o uvedbi novih storitev, postopkov ali tehnologij sem analizirala pod kodo G2– Nove storitve in postopki. Večina intervjuvancev (INT3, INT4, INT5, INT7, INT8) je poudarila, da zaradi zakonodaje o varstvu osebnih podatkov niso uvedli bistveno novih storitev ali tehnoloških rešitev. Dva intervjuvanca (INT1, INT6) sta ob tem izpostavila, da morebitni ukrepi niso bili namenjeni izključno varstvu osebnih podatkov, temveč širšemu varovanju vseh občutljivih podatkov, s katerimi se računovodski servisi vsakodnevno srečujejo. Kljub temu so nekateri intervjuvanci navedli določene spremembe v praksi, kot so podpisovanje pogodb in obveščanje novih strank o varovanju osebnih podatkov (INT1 in INT2), usposabljanje zaposlenih (INT1 in INT2), uvedba ali nadgradnja IT-rešitev (INT1), dodatna zaščita posameznih programskih modulov (INT2), urejanje in posodabljanje dokumentacije (INT1) ter doslednejše brisanje osebnih podatkov (INT2). Prav tako je en intervjuvanec (INT2) omenil večjo previdnost pri razkritjih osebnih podatkov. Ti odgovori kažejo, da so bile spremembe, povezane z zakonodajo, večinoma postopne in usmerjene v

izboljšanje že obstoječih praks, ne pa v uvajanje povsem novih storitev ali poslovnih modelov.

Odgovori intervjuvancev kažejo, da uvedba zakonodaje o varstvu osebnih podatkov ni bistveno posegla v vsakodnevne delovne procese računovodskih servisov. Vpliv zakonodaje se je pokazal predvsem na podpornih in administrativnih nalogah, medtem ko je vsakodnevno delo računovodskih servisov ostalo relativno nespremenjeno. To je mogoče deloma pripisati tudi dejstvu, da večina intervjuvanih še nima v celoti urejene vse predpisane dokumentacije. Spremembe, ki so jih servisi kljub temu uvedli, so bile večinoma postopne in usmerjene v splošno krepitev varnosti vseh občutljivih podatkov, s katerimi delajo, ne zgolj v varovanje osebnih podatkov.

5.2 Ugotovitve intervjujev in diskusija

V praktičnem delu magistrskega dela so bili s pomočjo analize predstavljeni rezultati globinskih intervjujev z računovodskimi servisi, ki osvetlijo dejansko stanje skladnosti z zakonodajo o varstvu osebnih podatkov v praksi. Analiza je omogočila sistematičen pregled obstoječih praks, zaznanih pomanjkljivosti in izzivov, s katerimi se računovodski servisi soočajo pri vsakodnevnem delu z osebnimi podatki. V nadaljevanju magistrskega dela sledi razprava, katere namen je s pomočjo teoretičnega okvirja in veljavne zakonodaje interpretirati ugotovitve iz analize.

Raziskava je pokazala, da manjši računovodski servisi v praksi delujejo v okolju, kjer se varstvo osebnih podatkov prepleta z vsakodnevnim poslovanjem, vendar pogosto ni obravnavano kot samostojno, sistematično urejeno področje. Ključna ugotovitev analize intervjujev je razkorak med zaznanim poznavanjem zakonodaje in dejansko stopnjo formalne skladnosti njenim zahtevam. Intervjuvanci so svoje poznavanje GDPR in ZVOP-2 večinoma ocenili kot srednje dobro do dobro, kar kaže na splošno zavedanje pomena varstva osebnih podatkov. Vendar rezultati analize razkrivajo, da to poznavanje pogosto ostaja na ravni osnovnih načel in izvajanja osnovnih, pretežno neformalnih previdnostnih ukrepov pri ravnanju z osebnimi podatki. Podrobnejše zakonske zahteve, zlasti glede ureditve ustrezne dokumentacije in bolj sistematična ureditev, kot so na primer določeni roki hrambe, opredelitev zbirk osebnih podatkov, določitev postopkov v primeru kršitev in jasno določena odgovornost med stranko in računovodskim servisom v pogodbi, pa pogosto niso implementirane.

Analiza intervjujev je pokazala, da večina računovodskih servisov nima formalno vzpostavljenih notranjih pravilnikov, jasno določenih postopkov za ravnanje v primeru kršitev ali uveljavljanja pravic posameznikov. Rezultati analize kažejo, da se računovodski servisi v veliki meri zanašajo na osebno odgovornost zaposlenih in ustaljene prakse, kar je sicer značilno za manjša podjetja, vendar ne zagotavlja zadostne ravni pravne varnosti. Na področju pogodbene ureditve s strankami se je pokazalo, da pogodbe o obdelavi osebnih podatkov pri večini intervjuvancev niso sklenjene. To predstavlja pomembno pomanjkljivost

z vidika 28. člena GDPR, ki izrecno določa obveznost sklenitve pisne pogodbe med upravljavcem in obdelovalcem. Empirični podatki nakazujejo, da računovodski servisi pogodbe o obdelavi osebnih podatkov pogosto dojemajo kot administrativno breme, ne pa kot ključen instrument za jasno razmejitev odgovornosti.

Raziskava je razkrila tudi več organizacijskih in vsebinskih izzivov, s katerimi se računovodski servisi soočajo pri zagotavljanju skladnosti. Pomanjkanje časa, dodatni stroški in administrativna obremenitev so najpogosteje navedeni razlogi za neurejeno dokumentacijo in pomanjkanje sistematičnega pristopa k varstvu osebnih podatkov. Kljub navedenim pomanjkljivostim rezultati analize kažejo, da zakonodaja o varstvu osebnih podatkov ni bistveno spremenila osnovnih delovnih procesov računovodskih servisov. Razlog za to utegne biti dejstvo, da večina računovodskih servisov nima urejene predpisane dokumentacije s tega področja. Vpliv zakonodaje se kaže predvsem v povečani previdnosti pri obdelavi osebnih podatkov in dodatni administraciji. To nakazuje, da je varstvo osebnih podatkov v računovodskih servisih pogosto integrirano v vsakodnevno delo na neformalen način. Celovito gledano analiza potrjuje razkorak med praktičnim ravnanjem z osebnimi podatki in pravnimi zahtevami zakonodaje. Računovodski servisi v večini primerov ravnajo odgovorno in zavestno, vendar njihova skladnost pogosto ni celovita oziroma se stopnja skladnosti med računovodskimi servisi tudi razlikuje.

6 SKLEP

Z uveljavitvijo GDPR in sprejetjem ZVOP-2 je varstvo osebnih podatkov postalo eno od ključnih pravnih in organizacijskih področij delovanja družb. Po mnenju Bajuk Mušič (2018) je nova ureditev okrepila pravice posameznikov in povečala odgovornost organizacije, Grgič (2017) pa dodaja, da je podjetjem naložila tudi dodatne obveznosti, ki se kažejo v večjem obsegu administrativnega dela, potrebi po usposabljanju zaposlenih ter dodatnih finančnih vložkih, zlasti v kontekstu digitalizacije in zagotavljanja ustrezne informacijske varnosti. Računovodski servisi pri svojem delu obdelujejo številne osebne podatke, predvsem zaradi izpolnjevanja zakonskih obveznosti (Bajuk Mušič, 2018). GDPR velja za vse organizacije, ki obdelujejo osebne podatke, zato morajo tudi računovodski servisi jasno opredeliti svojo vlogo – ali nastopajo kot upravljavci ali obdelovalci osebnih podatkov (ICAEW, 2018). Obdelava zajema vsa dejanja v zvezi z osebnimi podatki, od zbiranja do izbrisa (Bajuk Mušič, 2018). V praksi računovodski servisi osebne podatke obdelujejo predvsem na podlagi zakonskih obveznosti in pogodb s strankami (Informacijski pooblaščenec, 2024b), pri čemer gre najpogosteje za podatke o zaposlenih, podatke za obračun plač, davkov in prispevkov ter podatke na računih fizičnih oseb (Informacijski pooblaščenec, 2019). Na podlagi teoretičnega pregleda zakonodajnega okvirja in empirične analize, izvedene z globinskimi intervjuji v osmih manjših računovodskih servisih, v nadaljevanju skozi odgovore na raziskovalna vprašanja in presojo osnovne teze smiselno povezujem ključna teoretična izhodišča z rezultati raziskovalnega dela.

Raziskovalno vprašanje 1: Kakšne obveznosti predpisuje trenutna zakonodaja s področja varstva osebnih podatkov računovodskim servisom?

Splošna uredba o varstvu osebnih podatkov (GDPR) računovodskim servisom praviloma nalaga vlogo obdelovalca osebnih podatkov, zato morajo izpolnjevati obveznosti iz 28. člena GDPR, ki med drugim določa obveznost sklenitve pogodbe o obdelavi osebnih podatkov z upravljavcem, izvajanje ustreznih tehničnih ukrepov in obdelavo osebnih podatkov izključno po navodilih upravljavca. Poleg tega GDPR v 5. členu določa temeljna načela obdelave osebnih podatkov, kot so zakonitost, omejitev namena, najmanjši obseg podatkov, točnost, omejitev hrambe in integriteta ter zaupnost. Člen 32 GDPR dodatno nalaga obveznost zagotavljanju ustrezne ravni varnosti obdelave ob upoštevanju tveganj, narave in obsega obdelave. ZVOP-2 te zahteve dopolnjuje in podrobneje ureja nacionalne vidike varstva osebnih podatkov, zlasti v povezavi z nadzornimi postopki in s sankcijami. Teoretični pregled zakonodaje jasno kaže, da so obveznosti računovodskih servisov večplastne in zajemajo tako vsebinske kot tudi formalne zahteve, pri čemer ima dokumentacija ključno vlogo pri izkazovanju skladnosti.

Raziskovalno vprašanje 2: Kako se predpisi s področja varstva osebnih podatkov odražajo v delovnih procesih manjših računovodskih servisov?

Rezultati analize vprašanja A1 kažejo, da se manjši računovodski servisi v veliki meri zavedajo svoje odgovornosti pri ravnanju z osebnimi podatki in svoje poznavanje zakonodaje ocenjujejo kot srednje dobro do dobro. Kot je razvidno iz analize vprašanja G1, se v praksi predpisi o varstvu osebnih podatkov najpogosteje odražajo v povečani previdnosti pri obdelavi osebnih podatkov, omejevanju dostopa do podatkov in zanašanju na zaupanje v zaposlene. Analiza vprašanj sklopa D je pokazala, da večina tehničnih in organizacijskih ukrepov, ki jih izvajajo računovodski servisi, ni bila uvedena zaradi zahtev GDPR, temveč predstavljajo splošne varnostne ukrepe za zaščito vseh občutljivih podatkov. To nakazuje, da varstvo osebnih podatkov v praksi pogosto ni obravnavano kot ločeno ali sistematično urejeno področje, temveč del širšega varovanja poslovnih informacij. Pomembna ugotovitev na podlagi analize vprašanja G2 je tudi, da večina računovodskih servisov zaradi zakonodaje ni uvedla novih ali bistveno spremenila delovnih procesov. Eden izmed možnih razlogov za to je neobstoj dokumentacije, saj brez jasno opredeljenih notranjih pravilnikov in postopkov zahteve zakonodaje težje postanejo del vsakodnevnih procesov. To kaže na razkorak med zaznanim poznavanjem zakonodaje in njeno dejansko implementacijo v delovne procese.

Raziskovalno vprašanje 3: Kakšne so posledice zahtev, ki jih prinaša skladnost z zakonodajo o varstvu osebnih podatkov za manjše računovodske servise?

Na podlagi analize intervjujev je mogoče ugotoviti, da je na to raziskovalno vprašanje težko podati enoten in povsem neposreden odgovor. Razlog za to je dejstvo, da večina intervjuvanih računovodskih servisov ne izpolnjuje vseh zakonskih zahtev s področja

varstva osebnih podatkov, zlasti na področju ureditve dokumentacije, kot izhaja iz analize odgovorov na vprašanja B1, B4, C1 in F2. Posledično intervjuvanci v odgovorih na vprašanje G1 navajajo, da zakonodaja o varstvu osebnih podatkov ni bistveno vplivala na njihovo delo ali delovne procese. Rezultati analize vprašanj sklopa G kažejo, da računovodski servisi, ki zakonodajne zahteve uresničujejo predvsem na ravni povečane previdnosti pri obdelavi osebnih podatkov in neformalnih praks, posledic skladnosti ne zaznavajo kot izrazitih, ker niso uvedli novih postopkov ali formalnih prilagoditev. Nadalje analiza tega sklopa vprašanj kaže, da se pri računovodskih servisih, ki zakonodajne zahteve upoštevajo v večji meri in imajo bolj sistematično urejeno področje varstva osebnih podatkov, posledice skladnosti kažejo v povečanju administrativnih obremenitev, večji porabi časa ter dodatnih stroških, povezanih z urejanjem dokumentacije in s pogodbenimi razmerji. Varstvo osebnih podatkov je pogosto razumljeno kot dodatna obveznost ob že obstoječih računovodskih nalogah. Hkrati analiza vprašanja G1 kaže, da skladnost z zakonodajo praviloma ne posega bistveno v samo vsebino računovodskega dela, temveč vpliva predvsem na podporne in administrativne procese, kot sta vodenje dokumentacije in obveščanje strank. Ustrezno urejeno področje varstva osebnih podatkov lahko prispeva k večji pravni varnosti računovodskih servisov in h krepitvi zaupanja strank, vendar intervjuvanci teh koristi pogosto ne zaznavajo kot neposredno ali takojšno prednost.

Raziskovalno vprašanje 4: Katere so najpogostejše pomanjkljivosti v skladnosti dela manjših računovodskih servisov z zakonodajo s področja varstva osebnih podatkov?

Analiza odgovorov na vprašanja B1, B4, C1 in F2 je pokazala, da so najpogostejše pomanjkljivosti povezane s pomanjkanjem dokumentacije. Večina računovodskih servisov nima vzpostavljenih notranjih pravilnikov, urejenih pogodbenih razmerij s strankami, določenih zbirk osebnih podatkov, rokov hrambe, ocen tveganja ali jasno določenih postopkov v primeru kršitev. Te ugotovitve so posebej pomembne, saj načela odgovornosti 5. člena GDPR zahtevajo, da upravljavci in obdelovalci ne le ravnajo skladno z zakonodajo, temveč morajo to skladnost tudi dokazovati. Pomanjkanje dokumentacije tako ne pomeni nujno neustreznega ravnanja z osebnimi podatki, vendar bistveno zmanjšuje možnost dokazovanja skladnosti v primeru nadzora ali kršitve.

Raziskovalno vprašanje 5: Ali so delovni procesi manjših računovodskih servisov v skladu z zakonodajo varstva osebnih podatkov?

Rezultati analize vprašanj sklopa C, D in E kažejo, da delovni procesi računovodskih servisov niso v celoti skladni z zakonodajo o varstvu osebnih podatkov. Stopnja skladnosti se med posameznimi računovodskimi servisi razlikuje, pri čemer imajo nekateri bolj urejene procese in več formalnih elementov, drugi pa se zanašajo predvsem na neformalne prakse in osebno odgovornost zaposlenih. Analiza odgovorov na vprašanji C3 in C4 je pokazala, da večina intervjuvancev nima ustrezno urejenih zbirk osebnih podatkov – zbirke osebnih podatkov imata urejene le dva intervjuvanca. Nadzor nad roki hrambe je tako pri večini urejen precej neformalno, poenostavljeno in različno pri vsakem intervjuvancu. En

intervjuvanec se recimo zanaša na sprotno brisanje, trije so navedli brisanje ob prenehanju sodelovanja, šest jih je izpostavilo vračanje fizične dokumentacije, dva pa se opirata predvsem na računovodske predpise glede hrambe podatkov. Tudi analiza vprašanj sklopa D kaže, da imajo vsi intervjuvanci do določene mere uvedene tehnične in organizacijske varnostne ukrepe za zaščito osebnih podatkov, vendar se obseg ukrepov med posameznimi servisi razlikuje. Vsi imajo na primer zaklenjene pisarne ter zaščiten dostop do računalnikov in programov z gesli, medtem ko so le štirje navedli, da imajo vzpostavljen videonadzor, alarmni sistem in kontrolo pristopa. Prav tako so le trije intervjuvanci izpostavili uporabo dvofaktorske avtentikacije in antivirusnih programov. Pri analizi vprašanj E3–E5, ki se nanašajo na ravnanje v primeru zahtev posameznikov za uveljavitev njihovih pravic, je prav tako razvidna različna stopnja skladnosti delovnih procesov z zakonodajo. Večina intervjuvancev je navedla, da zahtevo posredujejo stranki oziroma predhodno pridobijo dovoljenje za njeno izpolnitev, pri čemer pa nobeden od intervjuvancev nima formalno določenih postopkov. Pri manjših računovodskih servisih so delovni procesi pogosto poenostavljeni, kar lahko prispeva k učinkovitemu in praktičnemu ravnanju z osebnimi podatki, hkrati pa pomeni manjšo sistematičnost. Takšen pristop je lahko v praksi deloma učinkovit, vendar ne zagotavlja popolne skladnosti z zakonodajnimi zahtevami zlasti glede dokumentiranja in obvladovanja tveganj.

Osnovna teza: Manjši računovodski servisi ustrezno ravnajo z osebnimi podatki svojih strank, vendar številni med njimi ne izpolnjujejo zahtev s področja zakonodaje o varstvu osebnih podatkov po izdelavi in vzdrževanju predpisane dokumentacije.

Na podlagi ugotovitev analize vprašanj sklopa C, D in E je mogoče osnovno tezo magistrskega dela delno potrditi. Analiza je pokazala, da računovodski servisi v večini primerov ustrezno in odgovorno ravnajo z osebnimi podatki svojih strank ter izvajajo osnovne varnostne ukrepe za njihovo zaščito. Kljub temu se stopnja skladnosti razlikuje med posameznimi računovodskimi servisi, kar pomeni, da raven ustreznega ravnanja z osebnimi podatki ni povsem enotna, zato ne moremo potrditi, da vsi računovodski servisi ustrezno ravnajo z osebnimi podatki svojih strank. Hkrati številni med njimi ne izpolnjujejo vseh zakonskih zahtev na področju izdelave, vodenja in vzdrževanja predpisane dokumentacije, kar predstavlja ključno pomanjkljivost z vidika zakonodajne skladnosti. Osnovno tezo lahko potrdimo v delu, kjer trdi, da številni računovodski servisi ne izpolnjujejo zahtev s področja zakonodaje o varstvu osebnih podatkov po izdelavi in vzdrževanju predpisane dokumentacije.

Rezultati izvedene raziskave kažejo, da manjši računovodski servisi v praksi večinoma ravnajo odgovorno in previdno pri obdelavi osebnih podatkov ter izvajajo osnovne tehnične in organizacijske ukrepe za njihovo varovanje. Kljub temu ugotovitve analize rezultatov, pridobljenih z globinskimi intervjuji, razkrivajo, da številni manjši računovodski servisi ne izpolnjujejo vseh formalnih zahtev, zlasti na področju izdelave, vodenja in vzdrževanja predpisane dokumentacije. Pomanjkanje notranjih aktov, urejenih pogodbenih razmerij in jasno določenih zbirk osebnih podatkov ter ustreznih rokov hrambe otežuje dokazovanje

skladnosti z zakonodajo, kar je v nasprotju z načelom odgovornosti, ki ga določa 5. člen GDPR. Ugotovitve magistrskega dela tako delno potrjujejo tezo o skladnosti dela manjših računovodskih servisov z zakonodajo o varstvu osebnih podatkov, vendar teze ni mogoče potrditi v celoti, saj ta skladnost ni enotna in v celoti zagotovljena. Osnovno tezo magistrskega dela je mogoče potrditi v delu, ki se nanaša na pomanjkljivosti pri zagotavljanju predpisane dokumentacije. Hkrati raziskava kaže, da bi bolj formaliziran pristop k varovanju osebnih podatkov lahko prispeval k večji pravni varnosti računovodskih servisov in k dolgoročni krepitvi zaupanja strank.

Nadaljnje raziskave bi bilo smiselno razširiti na večje računovodske servise ter primerjati stopnjo formalizacije in sistematičnosti pristopa k varstvu osebnih podatkov glede na velikost organizacije. Prav tako bi prihodnje študije lahko vključevale tudi kvantitativni pristop z večjim vzorcem podjetij ali primerjalno analizo med različnimi panogami, kjer organizacije nastopajo kot pogodbeni obdelovalci osebnih podatkov. Takšne raziskave bi omogočile širše razumevanje izzivov in dobrih praks ter prispevale k oblikovanju bolj ciljno usmerjenih poročil za izboljšanje skladnosti na področju varstva osebnih podatkov.

SEZNAM KLJUČNE LITERATURE

1. Bajuk Mušič, A. (2018). Varstvo osebnih podatkov v računovodstvu z vidika GDPR. *Revija za računovodstvo, davščine in finance*, 14–26.
2. Igličar, A., Hočevar, M., in Zaman Groff, M. (2017). *Osnove računovodstva*. Ekonomska fakulteta Univerze v Ljubljani.
3. Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). *Uradni list EU, št. L119/1.*
4. Xuereb, K., Bezzina, F. H., Farrugia, A., Grima, S., in Marano, P. (2019). The Impact of the General Data Protection Regulation on the Financial Services' Industry of Small European States. *International Journal of Economics and Business Administration,* 7(4), 243–266.
5. Zakon o Informacijskem pooblaščencu (ZInfP). *Uradni list RS, št. 113/05 in 51/07 – ZustS–A).*
6. Zakon o varstvu osebnih podatkov (ZVOP–2). *Uradni list RS, št. 163/22*.

LITERATURA IN VIRI

1. Abdalla, P. A., in Varol, A. (2019). Advantages to Disadvantages of Cloud Computing for Small–Sized Business. V *2019 7th International Symposium on Digital Forensics and Security (ISDFS),* (str. 1–6). https://doi.org/10.1109/ISDFS.2019.8757549
2. Bajuk Mušič, A. (2018). Varstvo osebnih podatkov v računovodstvu z vidika GDPR. *Revija za računovodstvo, davščine in finance*, 14–26.

3. Beaver, S. (2023, 24. oktober). *What Is Accounting? Definition, Types, History, in Examples. Oracle NetSuite.* https://www.netsuite.com/portal/resource/articles/accounting/accounting.shtml
4. Bodnarova, J. (2019, 13. maj). *GDPR one year on: Its impact on auditors and accountants? Accountancy Europe.* https://accountancyeurope.eu/stories/gdpr–one–year–on–its–impact–on–auditors–and–accountants/
5. Burke, J. A., in Polimeni, R. S. (2023, december 1). The Accounting Profession Is in Crisis. The CPA Journal. https://www.cpajournal.com/2023/12/01/the–accounting–profession–is–in–crisis/
6. Čadež, S. (2013). *Temelji poslovodnega računovodstva*. Ekonomska fakulteta Univerze v Ljubljani.
7. Data d.o.o. (2024, 10. september). *Pravilniki GDPR – ključni dokumenti, ki jih mora imeti delodajalec* [objava na blogu]. Pridobljeno 1. julija 2025 s https://data.si/blog/pravilniki–gdpr–kljucni–dokumenti–ki–jih–mora–imeti–delodajalec/
8. Data d.o.o. (2025, 4. junij). GDPR: *Ste skladni ali v prekršku? Preverite zdaj!* [objava na blogu]. Pridobljeno 1. julija 2025 s https://data.si/blog/gdpr-nasi-pravniki-opozarjajo/
9. Direktiva 2013/34/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o letnih računovodskih izkazih, konsolidiranih računovodskih izkazih in povezanih poročilih nekaterih vrst podjetij, spremembi Direktive 2006/43/ES Evropskega parlamenta in Sveta ter razveljavitvi direktiv Sveta 78/660/EGS in 83/349/EGS. *Uradni list EU, L 182, 29.6.2013, str. 19–76*
10. Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ. *Uradni list EU, L 119, 04.05.2016, str. 89–131.*
11. Direktiva 2006/43/ES Evropskega parlamenta in Sveta z dne 17. maja 2006 o obveznih revizijah za letne in konsolidirane računovodske izkaze, spremembi direktiv Sveta 78/660/EGS in 83/349/EGS ter razveljavitvi Direktive Sveta 84/253/EGS. *Uradni list EU, L 157, 09.06.2006, str. 87–107.*
12. Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. *Uradni list EU, L 281, str. 31–50.*
13. European Commission. (2025, 3. september). *Data protection explained. European Commission.* Pridobljeno 3. septembra 2025 s https://commission.europa.eu/law/law–topic/data–protection/data–protection–explained_en
14. GBPSSI. (brez datuma). *Concept of accounting. Gitarattan International Business School.* https://www.gbpssi.in/admin/coursepack/MBR517Lect01.pdf
15. Ministrstvo za finance. (2025, 7. avgust). *Javno računovodstvo. GOV.SI.* Pridobljeno 14. septembra 2025 s https://www.gov.si/teme/javno–racunovodstvo/
16. Grgič, M. (2017, 27. december). *Varstvo osebnih podatkov prinaša dodatne stroške. Svet kapitala.* Pridobljeno 3. septembra 2025 s https://svetkapitala.delo.si/ikonomija/varstvo–osebnih–podatkov–prinasa–dodatne–stroske/
17. ICAEW. (2018, junij). *GDPR for accountants: Your questions answered.* Pridobljeno 30. junija 2025 s https://www.icaew.com/–/media/corporate/files/technical/ethics/information–law–and–guidance/gdpr/faqs–what–does–gdpr–mean–for–accountants.ashx

18. Igličar, A., Hočevar, M., in Zaman Groff, M. (2017). *Osnove računovodstva*. Ekonomska fakulteta Univerze v Ljubljani.
19. Informa studio d.o.o. (2025). *Kaj bo za nas opravljal računovodja?* [objava na blogu]. Pridobljeno 1. julija 2025 s https://www.primerjam.si/nasveti/racunovodski–servis/kaj–bo–za–nas–opravljal–racunovodja
20. Informacijski pooblaščenec. (2019, 25. november). *Varstvo osebnih podatkov v delovnih razmerjih: Smernice Informacijskega pooblaščenca.* https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_-_Varstvo_OP_v_delovnih_razmerjih_verzija_1.1_koncna.pdf
21. Informacijski pooblaščenec. (2024a). *Evidenca dejavnosti obdelave—IPRS. Evidenca dejavnosti obdelave.* Pridobljeno 03. septembra 2025 s https://www.ip-rs.si/mnenja-gdpr/evidenca-dejavnosti-obdelave-1653558661
22. Informacijski pooblaščenec. (2024b). *Ključne novosti ZVOP–2. IPRS. Ključne novosti ZVOP–2.* Pridobljeno 02. januarja 2025 s https://www.ip–rs.si/zakonodaja/zakon–o–varstvu–osebnih–podatkov/zvop–2
23. IPRS. (2020, 20. marec). *Smernice Informacijskega pooblaščenca o (pogodbeni) obdelavi osebnih podatkov.* Pridobljeno 25. junija 2025 s https://www.ip–rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_pogodbeni_obdelavi_web.pdf
24. IPRS. (2025a, 3. januar). *Evropski okvir za varstvo podatkov. IPRS*. Pridobljeno 3. januarja 2025 s https://www.ip–rs.si/zakonodaja/reforma–evropskega–zakonodajnega–okvira–za–varstvo–osebnih–podatkov/
25. IPRS. (2025b, 7. junij). *Informacijska pooblaščenka. IPRS*. Pridobljeno 7. junija 2025 s https://www.ip–rs.si/o–poobla%C5%A1%C4%8Dencu/informacijska–poobla%C5%A1%C4%8Denka
26. IPRS. (2025c, 11. junij). *Varnost osebnih podatkov. IPRS.* Pridobljeno 11. junija 2025 s https://www.ip–rs.si/varstvo–osebnih–podatkov/obveznosti–upravljavcev/zavarovanje–oz–varnost–osebnih–podatkov
27. Jackson, D., Richardson, J., Michelson, G., in Munir, R. (2023). *The Future of Accounting Talent: Career Values, Choices and Satisfaction Among Early Career Accountants. Australian Accounting Review, 33(4),* 391–406. https://doi.org/10.1111/auar.12409
28. Jamšek, B. (2018, 20. november). *GDPR: Uredba o varstvu podatkov. Mladipodjetnik.si.* https://mladipodjetnik.si/novice–in–dogodki/novice/gdpr–uredba–o–varstvu–podatkov
29. Kamenšek, D. (2022, 30. maj). *Splošno o Mednarodnih standardih računovodskega poročanja. Unija ETL Smart Accounting.* https://unija.com/sl/splosno–o–mednarodnih–standardih–racunovodskega–porocanja/
30. Khanom, T. (2017). *Cloud Accounting: A Theoretical Overview. IOSR Journal of Business and Management (IOSR–JBM)*, 19(6), 31–38. https://doi.org/10.9790/487X–1906053138
31. Kovačevič, M. (2023, 20. februar). *Ključne novosti Zakona o varstvu osebnih podatkov – ZVOP–2. Razvojna agencija Sotla*. https://www.ra–sotla.si/kljucne–novosti–zakona–o–varstvu–osebnih–podatkov–zvop–2/
32. Kraigher Mišič, K. (2019, 16. oktober*). Hramba osebnih podatkov.* Uradni list. https://www.uradni–list.si/novice/pogled/hramba–osebnih–podatkov/hramba–osebnih–podatkov/hramba–osebnih–podatkov
33. La Torre, M., Botes, V. L., Dumay, J., in Odendaal, E. (2021). *Protecting a new Achilles heel: The role of auditors within the practice of data protection*. Managerial Auditing Journal, 36(2), 218–239. https://doi.org/10.1108/MAJ–03–2018–1836

34. Langeršek, E., in Brajnik, M. (2018, 16. maj*). GDPR v računovodstvu. Davki in računovodstvo* [objava na blogu]. https://www.dara.si/33/gdpr–v–racunovodstvu–uniqueiduchxzASYZNbkTqZZtTT5MoD646O3ij5x/
35. Lavinski, S. (2019, 21. julij). *10 Disadvantages in Risks of Cloud Computing. Medium*. https://faun.pub/10–disadvantages–risks–of–cloud–computing–35111de75611
36. Layton, L. (2020). *How to read a Financial Statement*. https://pdhonline.com/courses/p203/p203content.pdf
37. Lončar, M. (2009). *Računovodstvo in finančno poslovanje*. Konzorcij višjih strokovnih šol za izvedbo projekta IMPLETUM. https://resitve.sio.si/wp–content/uploads/sites/7/2019/11/Racunovodstvo_in_financno_poslovanje–Loncar.pdf
38. Mayr, B. (2017). *Osnove računovodstva*. Visoka šola za računovodstvo in finance.
39. Miller, S. (2022, 30. september). *What is an Accounting Firm? Capterra*. https://www.capterra.com/resources/what–is–an–accounting–firm/
40. Moudud–Ul–Huq, S., Asaduzzaman, M., in Biswas, T. (2020). *Role of cloud computing in global accounting information systems. The Bottom Line*, 33(3), 231–250. https://doi.org/10.1108/BL–01–2020–0010
41. Robnik, L. (2008). *Finančno računovodstvo*. https://www.skupnost–vss.si/impletum/docs/Skriti_dokumenti/Financno_racunovodstvo–Robnik.pdf
42. Schmidt, J. (2025). *Three Financial Statements. Corporate Finance Institute*. https://corporatefinanceinstitute.com/resources/accounting/three–financial–statements/
43. Slovenski inštitut za revizijo. (2016). Pravila skrbnega računovodenja (2016).
44. Slovenski računovodski standardi 2024. Uradni list RS, št. 129/23
45. Stanciu, V., in Rîndașu, S.–M. (2018). *The Impact of General Data Protection Regulation in The Accounting Profession – Evidences from Romania.* Journal of Information Assurance and Cybersecurity, 2018, 1–9. https://doi.org/10.5171/2018.758054
46. Teehan, H. (2025, 25. junij). *How will GDPR affect accountants? An update* [objava na blogu]. https://blog.caseware.co.uk/blog/gdpr–data–protection–regulation–update
47. Thomson Reuters Tax and Accounting. (2018, 7. januar). *Impact of GDPR on accountants.* Thomson Reuters Tax and Accounting – UK/EMEA. https://tax.thomsonreuters.co.uk/blog/impact–of–gdpr–on–accountants/
48. Tobin, J. M. (2025, 9. junij). *Basic Accounting Terms. Accounting.com.* https://www.accounting.com/resources/basic-accounting-terms/
49. Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). *Uradni list EU, L 119, 4.5.2016, str. 1–88.*
50. Uredba Komisije (EU) 2023/1803 z dne 13. avgusta 2023 o sprejetju nekaterih mednarodnih računovodskih standardov v skladu z Uredbo (ES) št. 1606/2002 Evropskega parlamenta in Sveta. *Uradni list EU, L 237, 26.9.2023, str. 1–992.*
51. Xuereb, K., Bezzina, F. H., Farrugia, A., Grima, S., in Marano, P. (2019). *The Impact of the General Data Protection Regulation on the Financial Services' Industry of Small European States.* International Journal of Economics and Business Administration, 7(4), 243–266. https://doi.org/10.35808/ijeba/342
52. Zakon o društvih (ZDru–1*). Uradni list RS, št. 64/11 – uradno prečiščeno besedilo in 21/18 – ZNOrg.*
53. Zakon o gospodarskih družbah (ZGD–1). *Uradni list RS, št. 65/09 – uradno prečiščeno besedilo, 33/11, 91/11, 32/12, 57/12, 44/13 – odl. US, 82/13, 55/15, 15/17, 22/19 – ZPosS, 158/20 – ZIntPK–C, 18/21, 18/23 – ZDU–1O, 75/23 in 102/24.*

54. Zakon o gospodarskih javnih službah (ZGJS). *Uradni list RS, št. 32/93, 30/98 – ZZLPPO, 127/06 – ZJZP, 38/10 – ZUKN in 57/11 – ORZGJS40.*
55. Zakon o Informacijskem pooblaščencu (ZInfP*). Uradni list RS, št. 113/05 in 51/07 – ZUstS–A.*
56. Zakon o javnih financah (ZJF). *Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13, 55/15 – ZFisP, 96/15 – ZIPRS1617, 13/18, 195/20 – odl. US, 18/23 – ZDU–1O, 76/23, 24/25 – ZFisP–1 in 39/25.*
57. Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT–2). *Uradni list RS, št. 48/22, 145/22, 17/25 in 56/25.*
58. Zakon o računovodstvu (ZR). *Uradni list RS, št. 23/99, 30/02 – ZJF–C in 114/06 – ZUE.*
59. Zakon o varstvu osebnih podatkov (ZVOP–1). *Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 177/20 – ZVOPOKD in 163/22 – ZVOP–2.*
60. Zakon o varstvu osebnih podatkov (ZVOP–2). *Uradni list RS, št. 163/22 in 40/25 – ZInfV–1.*
61. Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD). *Uradni list RS, št. 177/20.*
62. ZRS. (2025a, avgust 21). Kodeks članov Zbornice računovodskih servisov. Gospodarska zbornica Slovenije. https://www.gzs.si/zbornica_racunovodskih_servisov/vsebina/O–nas/Kodeks–ZRS
63. ZRS. (2025b, avgust 21). Zbornica računovodskih servisov. Gospodarska zbornica Slovenije. https://www.gzs.si/zbornica_racunovodskih_servisov/vsebina/O–nas/O–ZRS

PRILOGE

Priloga 1: Okvirna vprašanja za lastnike/zastopnike računovodskih servisov

Poznavanje zakonodaje	1. Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih? 2. Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?
Notranja politika v računovodskem servisu	3. Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov? 4. Glede na to, da nimate določenih zbirk osebnih podatkov, kako potem zagotavljate pregled nad tem katere osebne podatke obdelujete in kako z njimi ravnate? 5. Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov? 6. Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate? 7. Ste že razmišljali o tem, da bi vzpostavili pravilnik oz. notranjo politiko o varstvu osebnih podatkov? Kateri so razlogi, da tega še niste storili? 8. Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja? 9. Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)? 10. Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?
Pogodbena ureditev s strankami	11. Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov? Kaj je razlog, da nimate sklenjenih pogodb? 12. Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate? 13. Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki? 14. Kako pa se potem v praksi znajdete, ko pride do vprašanja, koliko časa je treba kakšne podatke hraniti?
Tehnični in organizacijski ukrepi v računovodskem servisu	15. Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov? 16. Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe? 17. Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

se nadaljuje

Priloga 2: Okvirna vprašanja za lastnike/zastopnike računovodskih servisov (nad.)

Skladnost z zakonodajo v praksi	18. Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj? 19. Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki? 20. Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)? 21. Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov? 22. Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas?
Izzivi	23. Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih? 24. Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate? 25. Ali imate morda narejeno oceno učinkov tveganja za zlorabo osebnih podatkov? 26. Če bi naredili oceno tveganja za zlorabo osebnih podatkov, kako bi ocenili, kje pri vas obstajajo največja tveganja in s kakšnimi vrstami tveganj se sploh soočate?
Vpliv zakonodaje	27. Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela? 28. Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Vir: lastno delo.

Priloga 3: Informacije o izvedbi intervjujev z lastniki/zastopniki računovodskih servisov

Oznaka intervjuja	Funkcija intervjuvanca in podatki o podjetju	Podatki o intervjuju
INT1	Zastopnica, lastnica v računovodskem podjetju s 4 zaposlenimi	Intervju opravljen 19. 09. 2025 v poslovnih prostorih podjetja v Kočevju
INT2	Zastopnica, lastnica v računovodskem servisu s 4 zaposlenimi	Intervju opravljen 03. 10. 2025 v poslovnih prostorih podjetja v Ribnici
INT3	Zastopnik, lastnik z 1–2 zaposlenimi	Intervju opravljen 07. 10. 2025 v kavarni v neposredni bližini poslovnih prostorov podjetja v Ljubljani
INT4	Zastopnik, solastnik v računovodskem servisu s 3–4 zaposlenimi	Intervju opravljen 10. 10. 2025 v poslovnih prostorih podjetja v Ljubljani
INT5	Zastopnica, lastnica v računovodskem servisu z 1–2 zaposlenimi	Intervju opravljen 06. 11. 2025 v kavarni v Kočevju
INT6	Zastopnica, lastnica v računovodskem servisu s 3 zaposlenimi	Intervju opravljen 11. 11. 2025 v poslovnih prostorih podjetja v Novem mestu
INT7	Zastopnica , lastnica v računovodskem servisu z 2 zaposlenima	Intervju opravljen 19. 11. 2025 v poslovnih prostorih podjetja na Brezovici
INT8	Zastopnica, lastnica računovodskega servisa z 9 zaposlenimi	Intervju opravljen 21. 11. 2025 v kavarni v neposredni bližini poslovnih prostorov podjetja v Kočevju

Vir: lastno delo.

Priloga 4: Transkript intervjuja INT1

A1 Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih?

Kar se nanaša na delo v računovodstvu, mislim, da dobro. Drugače pa če pride do situacije, ko imamo kakšno vprašanje ali nejasnost se raje obrnemo kar na pravnika, ki nam je uredil zadeve okoli varstva osebnih podatkov.

A6 Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?

Definitivno pogodba s stranko in obvestilo kakšne osebne podatke sploh obdelujemo. Potem vem, da smo morali takrat ko smo urejali to sprejeti tudi pravilnik o varstvu osebnih podatkov, določili smo tudi zbirke osebnih podatkov in oceno učinkov tveganja za zlorabo. Pa tudi zaposleni so podpisali izjave o varovanju osebnih podatkov. To je mogoče bolj kar se tiče »papirologije«, upam, da nisem še na kaj pozabila.
Na splošno bi pa rekla, da je pomembna varna hramba osebnih podatkov, zaščita dostopov z gesli, določanje in upoštevanje rokov hrambe in pa seveda tudi ozaveščanje in izobraževanje zaposlenih.

B1 Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov?

Obdelujemo tiste osebne podatke, ki so potrebni za izvajanje računovodskih in kadrovskih storitev – torej za obračun plač, prispevkov, pripravo pogodb, računov in podobno. To so recimo osnovni podatki kot so ime, priimek, naslov, davčna številka, EMŠO, e–poštni naslov, številka transakcijskega računa in podobno.

Potem zbirajo se osebni podatki za pripravo pogodb o zaposlitvi, podjemnih ali drugih oblik. Potem tudi podatki povezani z obračunom plač, prispevkov, nadomestil stroškov dela ter drugih prejemkov. Tudi podatki o delovnem času, bolniških odsotnostih in vzdrževanih družinskih članih. Pri dobaviteljih in kupcih naših strank pa tudi podatki iz računov, naročil in drugih poslovnih listin. Tako imamo določeno v naših zbirkah osebnih podatkov, ki jih imamo določene o naših zaposlenih in pogodbenih sodelavcih, o zaposlenih pri strankah in njihovih pogodbenih sodelavcih, o kupcih naših strank in o dobaviteljih strank, ki so fizične osebe.

B3 Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Ne nimamo, ker po zakonu nismo dolžni. Če se prav spomnim, je to za večja podjetja. Nas je zaposlenih med 3 in 4.

B4 Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate?

Imamo vzpostavljen pravilnik o varstvu osebnih podatkov. Posodobili ga še nismo odkar ga imamo. Smo ga pa sprejeli leta 2023. Smo hoteli prej pa enostavno ni bilo časa. Vsa priprava dokumentov oz. pogodb in pridobivanje podpisov pogodb s strani strank je trajala več kot en mesec. Imamo namen posodabljati vsakih nekaj let oz. ko bo prišlo do kakšnih večjih sprememb.

B6 Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja?

Ja, izvajamo redna letna usposabljanja. Jaz jih vodim. Najprej sama preučim, če je kaj novega, potem pa gremo skupaj čez. Res je, da to niso prav neki tečaji ali seminarji, ampak za vse zaposlene bi bilo to enostavno predrago in preveč časovno potratno. Poleg tega pa to ni edina stvar glede katerih se morajo zaposleni izobraževati.

B7 Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)?

Načeloma imam ekipo, ki ji lahko precej zaupam, da delajo v skladu s pravili. Tako da preverjam jih načeloma niti ne. Vsaj ne prav namensko oziroma načrtno. Ampak, ker smo manjše podjetje, imam bolj ali manj vse pod kontrolo in mislim, da bi hitro opazila, če kaj ne bi bilo v redu. Glede motivacije pa tudi ne vem kaj bi izpostavila. Mogoče predvsem opozorila, ampak kot sem že rekla me zaposleni pridejo vprašat, če glede česa niso prepričani, drugače pa kar dobro vedo kaj smejo in česa ne.

B8 Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?

Pripravljen imamo obrazec oz. predlogo »obvestilo o kršitvi varstva osebnih podatkov posameznika«. V primeru kršitve bi ta obrazec izpolnili in poslali naši stranki, da ukrepa naprej in obvesti posameznika.

C1 Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov?

Ja imamo. Sklenili smo jih leta 2023 z vsemi, ko smo sprejeli pravilnik o varstvu osebnih podatkov, z novimi strankami pa zdaj pogodbe pripravljamo in podpisujemo sproti.

C2 Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate?

Ne, glede samega našega dela ne vodimo evidence, ker za nas to ni zakonsko obvezno. Vodimo edino evidenco vpogledov za videonadzor. Zaradi varnosti imamo namreč v poslovnih prostorih tudi kamere.

C3 Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki?

Rok hrambe dokumentacije imamo določen v zbirkah osebnih podatkov. Roke hrambe je določil pravnik, ki nam je vso dokumentacijo pripravljal, sama priznam, da se nisem poglabljala v to kakšni morajo biti te roki, glede tega zaupam našemu pravniku. Je pa dobro, da smo jih določili, ker smo poslovanje nekoliko bolj digitalizirali. Včasih smo papirje v celoti vrnili stranki ob končani bilanci in s tem ni bilo težav, zdaj pa je veliko več skeniranega in je potrebno veliko bolj paziti, da zadeve brišemo. Načeloma imamo za Zbirke osebnih podatkov o zaposlenih pri strankah in pogodbenih sodelavcih strank obdobje hrambe »dokler za stranko izvajamo računovodske storitve«, pri zbirkah osebnih podatkov o naših zaposlenih in zbirkah o naših pogodbenih sodelavcih je obdobje hrambe »trajno« in pri zbirkah osebnih podatkov o dobaviteljih do strank, ki so fizične osebe ter kupcih do strank »dokler za stranko izvajamo računovodske storitve oz. dokler se osebni podatki ne predajo stranki v hrambo«. Nekega posebnega nadzora nad roki pa nimamo. Mislim, da imamo te roke precej široko zastavljene. Pazimo morda predvsem, da če prenehamo poslovati z neko stranko zbrišemo vso dokumentacijo, ki je v elektronski obliki, fizično dokumentacijo pa vrnemo.

D1 Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov?

Za namen varovanja prav osebnih podatkov nismo uvedli nič specifičnega, razen mogoče, da smo sprejeli vso potrebno dokumentacijo in bolj izobrazili zaposlene. Moramo pa na sploh poskrbeti za varnost podatkov, ker delamo z veliko količino podatkov, ki so občutljive narave, tudi če niso to ravno osebni podatki. S tem namenom imamo kamere, zaklenjena vhodna vrata z videofonom, da lahko pred vstopom osebe preverimo kdo pride notri. Potem imamo tudi računalnike in programe zaščitene z gesli, antivirusni program, rekla bi da sem sodi tudi 24–urna podpora informatika, ki res skrbi, za visok nivo varnosti vseh naših podatkov. Priznam, da ta del vseeno tehnično ne poznam toliko, da bi bolj točno odgovorila na to vprašanje. Tako kot dokumentacijo zaupam pravniku, ta del zaupam našemu informatiku.

D2 Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe?

Tako kot sem že povedala pri prejšnjem vprašanju. Mogoče še nekako najbolj z gesli. Recimo pri modulu plač je drugačno geslo kot je pri modulu glavne knjige. Smo pa manjše podjetje, tako da imamo od zaposlenih načeloma vsi dostop do podatkov, ki jih potrebujemo za opravljanje svojega dela. Imamo tudi tako določeno v sprejetem pravilniku o varstvu osebnih podatkov, da imajo vsi zaposleni dostop do osebnih podatkov, ki jih potrebujejo za

opravljanje svojega dela, jaz kot direktor imam pa polni dostop. Bi pa izpostavila, da smo zaposlene samo res zaupanja vredne osebe. Morda le občasno kakšen študent, ki pride pomagati skenirati ob povečanem obsegu dela nima dostopa do vsega – mu ne povemo gesel do modula plač in pozna samo geslo na tistem računalniku kjer ima omejen dostop do podatkov.

D3 in D4 Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

Ponekod imamo vzpostavljeno dvofaktorsko prijavo, mislim, da predvsem v bankah za namene plačevanja. Tudi nekatere dokumente, ki jih pošiljamo preko e pošte imamo šifrirane, na primer plačilne liste. Izvajamo tudi dnevne varnostne kopije vseh podatkov, ne samo osebnih. Vsak dan se ponoči samodejno zažene backup, en se shrani tukaj na lokaciji podjetja, drugi pa na drugi varni lokaciji. Dostop imam samo jaz in naš računalničar oz. informatik. Ampak imamo narejeno tako, da ima dostop preko mene, tako da sam ne more kar prosto dostopati do podatkov. Potem pa jaz recimo enkrat tedensko naredim še backup na zunanji trdi disk, ki je pa spet hranjen še na tretji varni lokaciji. Tako da v bistvu imamo za varnost podatkov res poskrbljeno.

E1 Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj?

Rekla bi, da smo kar skladni na vseh področjih. Mogoče edino to, da ne posodabljamo vse dokumentacije iz tega področja vsako leto.

E2 Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki?

Ne, nismo imeli.

E3 Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)?

Takega primera sicer še nismo imeli, da bi določen posameznik zahteval uveljavitev svojih pravic. Mi v prvi vrsti tako ali tako komuniciramo s stranko oz. z osebo, ki jo stranka pooblasti za komunikacijo z nami tako da z zaposlenimi strank, njihovimi kupci, dobavitelji, poslovnimi partnerji in podobno nimamo stikov. Smo pa vsem strankam ob podpisu pogodbe o varstvu osebnih podatkov dali še obvestilo o varstvu in obdelavi osebnih podatkov na katerem jasno pišejo vse njihove pravice, tako da so z njimi dobro seznanjeni.

E4 Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

V primeru, da recimo do nas pristopi zaposleni naše stranke, in želi denimo svoje plačilne liste, spremembo naslova, TRR–ja in podobno, mu mi žal ne moremo ugoditi. Mi imamo stik samo s stranko neposredno, oz. z osebno ki je s strani stranke pooblaščena za komunikacijo z nami. Posameznik komunicira s svojim delodajalcem – našo stranko, ki potem obvesti nas kaj potrebuje. Pri izbrisu je pa po navadi tako, da za večino osebnih podatkov obstaja zakonska obveznost hrambe in je posledično verjetno niti ne bi mogli uveljavljati. Takega primera niti še nismo imeli.

E5 Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas, čeprav v praksi običajno nimate stika z njimi?

Ne vem če temu lahko rečemo postopek, ampak vsi zaposleni vedo, da neposredno z zaposlenim strank ali recimo njihovim strankam, dobaviteljem, ne smejo razkrivati nikakršnih podatkov. Ne osebnih, ne kakšnih drugih občutljivih. V primeru, da pride do takšne situacije potem kontaktiramo stranko. Poleg tega imajo pa vedno, glede vsega moji zaposleni navodilo, da če glede česa niso prepričani stoodstotno, vedno pridejo vprašati mene.

F1 Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih?

Mislim, da predvsem čas, ki je potreben, da vse skupaj urediš. Pa tudi stroški. Kot prvo potrebuješ kar nekaj časa, da pripraviš vse pogodbe, da pridobiš podpise s strani strank. Nekatere stranke so ažurne in hitro vse uredijo, potem druge pa prosiš in prosiš, da vrnejo podpisane pogodbe. Potem tudi strošek ni ravno zanemarljiv. Nas je nekaj stal pravnik, da je pripravil vso dokumentacijo potem pa še en dober mesec dela zaposlenega oziroma zaposlenih, ki ga je bilo potrebno plačati, da se je vse skupaj pripravilo.

F2 Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate?

Da, mislim, da imamo vse, glede na to, da nam je vse skupaj pripravil pravnik.

G1 Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela?

Mislim, da moramo biti predvsem na splošno bolj pazljivi, glede razkrivanja osebnih podatkov. Zaposlene je potrebno izobraževati, da vedo kaj smejo in česa ne. Včasih bi kakšna stranka rada kaj kar po domače pa ne smeš in jim moraš potem razložiti, da to ne gre tako.

G2 Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Težko rečem, da smo uvedli kaj na novo prav zaradi ZVOP–2 ali GDPR. Mogoče redno usposabljanje zaposlenih, potem za nove stranke pripravimo pogodbo o varstvu osebnih

podatkov za podpis in obvestilo o varstvu osebnih podatkov, da jih seznanimo z njihovimi pravicami, namenom obdelave in kdo ima dostop do njihovih osebnih podatkov. Drugače kar se tiče varstva podatkov moramo pa mi v vsakem primeru poskrbeti za varnost, ker poleg osebnih podatkov obdelujemo veliko občutljivih podatkov, ki niso vedno osebni.

Priloga 5: Transkript intervjuja INT2

A1 Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih?

Rekla bi, da kar dobro. V našem poklicu je skoraj nujno, da si redno na izobraževanjih in seminarjih, kjer poleg drugih tem občasno pridejo na vrsto tudi vsebine o varstvu osebnih podatkov. Poleg tega imamo naročene tudi strokovne revije in e–novice, kjer sproti objavljajo spremembe in novosti. Tako da sem kar v toku, čeprav seveda vedno ostane prostor za izboljšave, ker se zakonodaja hitro spreminja.

A6 Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?

Najbolj pomembno je, da so podatki varno shranjeni in zaščiteni pred nepooblaščenimi dostopi. Potem pa, da zaposleni dobro vedo kaj smejo in česa ne smejo početi – torej ustrezno usposabljanje. Ključno je tudi, da imamo urejeno vso potrebno dokumentacijo, da zmanjšajmo neko pravno izpostavljenost.

B1 Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov?

Obdelujemo osebne podatke, ki jih nujno potrebujemo za računovodske in kadrovske storitve – torej za obračun plač, prispevkov, pripravo pogodb, računov in podobno. TO so običajno ime, naslov, EMŠO, davčna številka, TRR in podobni osebni podatki. Potem pa tudi osebni podatki, ki se znajdejo na različnih pogodbah kot so avtorske pogodbe, podjemne pogodbe, občasno delo in druge. Imamo tudi eno stranko, rokometno društvo, pri katerem moramo za vse člane pridobiti osebne podatke, da lahko oddamo podatke za odmero dohodnine za razne prevoze z avtobusom, ki jih financira društvo. V tem primeru moramo od vsakega člana pridobiti ime in priimek ter davčno številko. Sicer moramo te podatke pridobivati pri vseh društvih ob izplačilu raznih štipendij, kilometrin in podobo, ampak v tem primeru, ko gre za nek rokometni klub, kjer je veliko članov teh osebnih podatkov kar nanese.

Glede zbirk osebnih podatkov, imamo zbirke o naših zaposlenih in pogodbenih sodelavcih, pa tudi o zaposlenih naših strank in njihovih pogodbenih sodelavcih ter o njihovih kupcih in dobaviteljih, ki so fizične osebe.

B3 Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Ne, nimamo.

B4 Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate?

Ja, notranji pravilnik imamo. Sprejeli smo ga pred približno enim letom, od takrat ga še nismo posodobili. Po mojem ga bomo posodabljali vsakih nekaj let, razen če bi prišlo do kakšnih večjih sprememb v zakonodaji. Pogoste spremembe so namreč kar strošek, zato poskušamo ravnati tudi malo racionalno.

B6 Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja?

Jaz redno hodim na usposabljanja in seminarje, potem pa pomembne novosti prenesem naprej sodelavcem. Na splošno pa so zaposleni dobro seznanjeni z osnovami, kaj lahko in kaj ne, tako da večjih težav na tem področju nismo imeli.

B7 Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)?

Jih ne preverjam. V praksi deluje tako, da če pride do kakšne konkretne situacije, se o tem odkrito pogovorimo. Imamo odprto komunikacijo, tako da le komu kaj ni jasno raje vpraša, kot da bi naredil napako. Do tega, da bi bilo treba koga kaznovati še ni prišlo – večinoma zadošča opozorilo na kaj je treba biti pozoren.

B8Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?

Posebnega postopka nimamo zapisanega. Če bi se zgodila takšna napaka, bi vsekakor obvestili stranko, da lahko tudi sama ustrezno ukrepa in obvesti prizadeto osebo.

C1 Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov?

Ne z vsemi. Imamo že pripravljen osnutek pogodbe, ampak moram priznati, da jih še nisem uspela razposlati čisto vsem strankam. To je nekaj, kar nas še čaka. Enostavno še ni bilo dovolj časa.

C2 Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate?

Ne, tega ne vodimo.

C3 Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki?

V pravilniku imamo določeno, da se podatki hranijo do konca pogodbenega razmerja ali do vračila dokumentacije. Za zaposlene pa se podatki povezani s plačami hranijo trajno, tako kot se po zakonu tudi morajo. Pri večini strank se dokumentacija po bilancah vrne, tako, da pri nas ne ostane. Za stranke, kjer je več dokumentacije v digitalni obliki, pa podatke ob prenehanju sodelovanja izbrišemo.

D1 Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov?

Uporabljamo gesla na računalnikih in programih, pisarno zaklepamo, prav tako tudi omare, kjer hranimo dokumentacijo.

D2 Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe?

Tako, da imamo na vsakem računalniku in programu geslo, ki ga poznajo samo tisti, ki ga smejo uporabljati. Pa recimo tudi ključa od pisarne nima vsak zaposleni, ga dobijo samo tisti, ki so pri nas že dalj časa in vem, da jim lahko zaupam. Kadar imamo recimo kakšno študentsko pomoč, ne dobijo ključa od pisarn.

D3 in D4 Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

Za dvofaktorsko prijavo ne vem, če imamo kje. Imamo pa šifrirane plačilne liste, ki jih pošiljamo preko e–pošte. Podatke varnostno kopiram približno enkrat tedensko na zunanji disk, do katerega imam dostop samo jaz. Hranim ga na drugi lokaciji, da v primeru vloma ali požara ne bi izgubili podatkov.

E1 Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj?

Po mojem, smo kar skladni, razen tega, da nimamo še urejenih pogodb z vsemi strankami.

E2 Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki?

Ne nismo še imeli.

E3 Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)?

Za zdaj še nismo imeli takšnega primera. Če bi prišlo do tega, bi ravnali tako, da je v skladu z zakonom. Če ne bi bili prepričani kaj je prav, bi se pozanimali tudi pri pravniku, ker se zavedamo, da so to občutljive zadeve. Načeloma pa mi obdelujemo podatke na podlagi

izpolnjevanja zakonskih zahtev in komuniciramo neposredno z našimi strankami. Z osebami na katere se osebni podatki nanašajo nimamo neposrednega kontakta. Tako da kakršna koli takšna zahteva mora priti s strani podjetja, ki je naša stranka.

E4 Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

Najprej bi kontaktirali našo stranko in pridobili njeno dovoljenje.

E5 Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas, čeprav v praksi običajno nimate stika z njimi?

V takem primeru vedno kontaktiramo našo stranko. Če zaposleni ne vedo kaj storiti, se obrnejo name in skupaj rešimo situacijo.

F1 Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih?

Največji izziv bi rekla, da je birokracija – vsa ta dodatna dokumentacija, pogodbe, pravilniki. Ker sami tega ne znamo pripraviti, je treba najeti pravnika, potem pa vse podatke vnesti, podpisati pogodbe in hraniti, obnavljati in podobno. To delo nam ne prinese nobene dodane vrednosti, hkrati pa ga moramo delati poleg rednega računovodskega dela, ki ga je že tako veliko in tudi vedno več.

F2 Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate?

Večinoma jo imamo, manjka pa še del pogodb s strankami.

F3 Ali imate morda narejeno tudi oceno učinkov tveganja za zlorabo osebnih podatkov?

Ja imamo tudi to ja, je prej nisem omenila. Povsod imamo ocenjeno nizko tveganje in nizko verjetnost. Možna tveganja pa so nepooblaščeni dostop, zloraba podatkov, predolga hramba, napačni podatki in podobno.

G1 Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela?

Na sam proces dela mislim, da ni vplivala veliko, razen, da moraš biti bolj pazljiv pri razkritjih in, da je več birokracije. Nekatere stvari moraš pač urediti dodatno, kar vzame čas.

G2 Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Ob pridobitvi vsake nove stranke podpisujemo pogodbo o varstvu osebnih podatkov. Potem programski modul za plače smo dodatno zaščitili z drugačnim geslom, kot druge module. Pa

tudi bolj smo dosledni pri brisanju podatkov in skrbimo, da ne pride do nepotrebnih razkritij. Zato je tudi pomembno, da so zaposleni dobro seznanjeni z zakonskimi zahtevami.

Priloga 6: Transkript intervjuja INT3

A1 Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih?

Če sem čisto iskren – zakonov konkretno nisem bral. Bi rekel, da jih ne poznam najbolje. Imam pa vseeno neko osnovno predstavo o tem kaj od nas zahteva zakonodaja in kaj je pomembno da kot računovodski servis upoštevamo. Se pravi – da podatkov ne delimo naprej, da jih varujemo tako fizično kot v digitalni obliki in da se uporabljajo samo za namen za katerega so bili pridobljeni.

A2 Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?

Najbolj ključno je, da so podatki dobro zaščiteni in da osebe, ki z njimi delajo vedo kaj je dovoljeno in na kaj morajo paziti. Se pravi neka osnovna skrbnost, da podatki ne pridejo v napačne roke in da do njih nima vsak dostopa.

Kaj pa recimo ureditev potrebne dokumentacije, kot so pravilnik o varstvu osebnih podatkov pogodbe o obdelavi s strankami, določitev zbirk osebnih podatkov, ocene tveganja in podobno?

To je sicer zakonsko obvezno in je prav, da bi to vsi imeli, ampak žal tu ne vidim dodane vrednosti za kakovost našega dela v računovodstvu. Le dodatno birokracijo in stroške.

B1 Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov?

Največkrat gre za podatke v povezavi z obračunom plač, podjemnimi pogodbami, avtorskimi pogodbami, kratkotrajnim delom družinskih članov, torej ime priimek, naslov, davčna številka, TRR in podobno. Formalno določenih zbirk osebnih podatkov pa nimamo.

Na koga se pa nanašajo osebni podatki, ki jih zbirate? Vaše zaposlene, stranke, njihove stranke?

Ja, na vse naštete. Morda je še najmanj osebnih podatkov pri strankah naših strank, razen kadar gre recimo za izdajo računov fizičnim osebam.

B2 Glede na to, da nimate določenih zbirk osebnih podatkov, kako potem zagotavljate pregled nad tem katere osebne podatke obdelujete in kako z njimi ravnate?

Res je, da nimamo nekega zelo sistematičnega pregleda v smislu določenih zbirk osebnih podatkov. Do neke mere nam pregled omogoča računovodski program, kjer imamo shranjeno praktično vse. V programu se tudi vidi, kdo je kdaj dostopal do podatkov. Posebej

pazimo, da osebne podatke res uporabimo samo za tisto, za kar so nam bili poslani, na primer za obračun plače ali pripravo pogodbe ipd. Če pridejo po mailu, jih po vnosu v program izbrišemo. Pa tudi da do njih ne dostopajo neke osebe, ki niso vredne zaupanja.

B3 Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Ne, nimamo. Sva samo dva zaposlena.

Ste mnenja, da bi morali imeti imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Mislim, da ne. Če se prav spomnim, je to za javna in večja podjetja.

B4 Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate?

Ne, nimamo nič od tega.

B5 Ste že razmišljali o tem, da bi vzpostavili pravilnik oz. notranjo politiko o varstvu osebnih podatkov? Kateri so razlogi, da tega še niste storili?

Enkrat bomo verjetno to morali urediti, ampak zaenkrat nekega resnega namena še nimamo. Res je, da je to zakonsko obvezno in bi bilo prav, da imamo to urejeno, ampak ne verjamem, da bo to naše delo izboljšalo ali kakorkoli drugače kaj doprineslo. Predstavlja pa to vseeno nek strošek, saj moramo nekoga plačati, da nam to pripravi, poleg tega pa je to tudi časovno potratno. Tako, da vam ve vem povedati kdaj se bomo tega lotili.

B6 Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja?

Ne izvajamo nekih posebnih usposabljanj. Smo naročeni na kar nekaj različnih e–novic, ki se nanašajo na delo računovodij, tako da potem dobimo na mail obvestila kjer pišejo aktualne novosti in je potem občasno tudi tam kaj objavljeno okoli varstva osebnih podatkov.

Bi ocenili, da so vaši zaposleni dobro seznanjeni s postopki glede varstva osebnih podatkov?

Ja, mislim, da ja.

B7 Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)?

Načeloma ne preverjam. Sva samo dva in načeloma me sodelavka vpraša, če glede česa ni prepričana, potem pa skupaj rešujeva naprej če še vedno ne veva kaj je prav.

B8 Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?

Ne, nimamo nobenega posebnega protokola. V primeru, da bi prišlo do neke hujše kršitve bi o tem obvestili našo stranko, potem pa bi skupaj poskušali rešiti nastalo situacijo.

C1 Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov?

Ne, nimamo.

Kaj pa je razlog, da nimate sklenjenih pogodb, če smem vprašati?

Razlog je enak kot pri pravilniku. Kot prvo mora nekdo pripraviti osnutek te pogodbe, potem jih je treba prirediti za podpis z vsako stranko posebej, tudi to mora spet nekdo narediti. Vse to stane in vzame kar nekaj časa.

C2 Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate?

Ne, ne vodimo.

C3 Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki?

Posebej določenih rokov hrambe nimamo. Načeloma niti ne hranimo prav veliko podatkov nikjer na lastnih računalnikih, ampak je vse shranjeno v programu do katerega dostopamo v brskalniku. Seveda ne morem zagotoviti, da nimamo pri sebi ničesar shranjenega, ampak se tega čim bolj izogibamo. Tudi arhiviranje plačujemo oz. plačuje stranka pri ponudniku programa. Kadar dobimo pa recimo mail, ki vsebuje podatke o novem delavcu pri stranki, ga po vnosu v program izbrišemo sproti.

C4 Kako pa se potem v praksi znajdete, ko pride do vprašanja, koliko časa je treba kakšne podatke hraniti?

V bistvu to prepustimo stranki. Ko so podatki enkrat arhivirani, torej po bilanci, mi načeloma ne dostopamo več do jih. Kaj pa stranka počne z njimi pa ne vem. Večji del osebnih podatkov, ki jih obdelamo so tako ali tako plače, ki jih morajo po zakonu hraniti trajno, za ostalo pa ne vem kako imajo urejeno.

D1 Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov?

Nič posebnega. Imamo zaklenjene pisarne, pod alarmom. Gesla na računalnikih in za v programe.

D2 Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe?

Z zaščitnimi gesli na računalnikih in v računovodskemu programu.

D3 in D4 Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

Dvofaktorske prijave nimamo. Po e–pošti pošiljamo šifrirane plačilne liste. Rednega varnostnega kopiranja podatkov pa ne izvajamo, ker imamo dostop do vseh podatkov preko brskalnika, tako, da mi nekih podatkov sploh ne hranimo. Hranimo osebne podatke o zaposlenih v našem podjetju, to tako ali tako moramo. Za stranke pa je v bistvu tako, da imajo oni dostop do programa v brskalniku in gor naložijo vse dokumente in podatke. Edino kar moramo paziti je, če recimo občasno dobimo mail s kakšnimi osebnimi podatki zaposlenega pri naši stranki, da ga potem izbrišemo, ko podatke vnesemo v program. Dostop do teh osebnih podatkov imajo potemtakem torej programerji iz minimaxa, mi v računovodstvu in naša stranka.

E1 Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj?

Trudimo se biti čim bolj, vsaj z vidika našega dela, ki ga opravljamo, ampak definitivno pa nimamo pravno urejenega tega področja. Torej nimamo sprejete in urejene vse potrebne dokumentacije.

E2 Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki?

Ne, še nikoli

E3 Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)?

Nisem še imel primera, kjer bi prišlo do takšnih zahtev.

E4 Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

Zdaj če gre to za nekega posameznika, ki je zaposlen pri naši stranki, ali ki je kupec/stranka naše stranke potem mi z njim itak ne smemo imeti kontakta. Jim kar povemo, naj se najprej obrnejo na našo stranko, potem pa nam da stranka navodila katere podatke želijo popraviti ali do katerih podatkov želijo dostopati. Izbrisati jih pa kar tako niti ne moremo. Sploh pri plačah. Jih moramo hraniti trajno po zakonu.

E5 Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas, čeprav v praksi običajno nimate stika z njimi?

Nimamo nobenega postopka.

F1 Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih?

Čas in denar, ki sta potrebna za pripravo vse potrebne dokumentacije, da podjetje lahko deluje v skladu z zakonodajo na tem področju.

F2 Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate?

Ne, nimamo nobene dokumentacije. Zagotovo bi morali imeti sklenjene pogodbe s strankami, potem verjetno tudi sprejet kakšen interni akt, ampak to vse stane in tudi nekaj časa ti vzame.

F3 Ali imate morda narejeno oceno učinkov tveganja za zlorabo osebnih podatkov?

Ne, nimamo ničesar.

F4 Če bi naredili oceno tveganja za zlorabo osebnih podatkov, kako bi ocenili, kje pri vas obstajajo največja tveganja in s kakšnimi vrstami tveganj se sploh soočate?

Na splošno bi ocenil, da so tveganja zelo majhna. Morda bi še nekako najbolj izpostavil tveganje, da podatki pomotoma pridejo do napačne osebe – na primer pošlješ mail napačni osebi ali pa narediš napako pri vnosu v program. Obstajajo pa vedno tudi tveganja, da do podatkov dostopajo nepooblaščene osebe, da jih neupravičeno hranimo in podobno.

G1 Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela?

Načeloma ni bistveno. Rekel bi, da je to še ena dodatna stvar glede katere se je potrebno izobraževati. Potem je pa tudi malo več usklajevanja s sodelavko, kaj je prav in kaj ne. Torej malo bolj moraš paziti, da recimo izbrišeš mail z osebnimi podatki zaposlenega stranke, ko jih enkrat vneseš v program in podobno. Skratka bolj moraš biti pazljiv.

G2 Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Mislim, da nismo.

Priloga 7: Transkript intervjuja INT4

A1 Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih?

Svoje poznavanje bi ocenila kot srednje dobro. Osnovne principe GDPR in ZVOP–2 poznam in jih pri svojem delu tudi upoštevam. Predvsem v smislu varnega ravnanja z osebnimi podatki strank in zaposlenih. Vem pa, da gre za zelo obsežno in dinamično področje, kjer se zakonodaja in razlage pogosto dopolnjujejo. Je pa tako, da mi v računovodstvu pokrivamo zelo širok nabor področij, ki so živa in se neprestano spreminjajo ter dopolnjujejo – na primer kadrovske zadeve, davki, priprava poročil itd.. Torej obstaja še veliko drugih področij na katerih se moramo izobraževati in v praksi imajo ta področja pogosto prednost.

A2 Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?

Po mojem mnenju je za računovodske servise najpomembnejša predvsem skrbnost pri ravnanju z osebnimi podatki. To pomeni, da moramo ves čas paziti, da ne pride do nenamernih razkritij podatkov in pa da so osebni podatki dostopni samo pooblaščenim osebam, ki pa s temi podatki tudi znajo pravilno ravnati, saj je po navadi ravno človeški faktor tisti, ki lahko najhitreje povzroči napako. Pomembno je tudi, da so ustrezno zaščiteni, fizični in v elektronski obliki pa tudi, da jih ne uporabljamo za neke druge namene ampak samo za tiste, za katere smo jih prvotno pridobili.

B1 Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov?

Pridobivamo predvsem osnovne osebne podatke kot so ime in priimek, EMŠO, davčna številka, naslov, telefonska številka, e–mail naslov, drugega bi rekla da niti ne. Aha še podatki o bančnem računu. To so podatki, ki jih potrebujemo predvsem v okviru priprave obračunov plač in drugih kadrovsko–računovodskih storitev. Občasno se osebni podatki pojavijo tudi na izdanih računih fizičnim osebam ali pa morda v kakšnih kupoprodajnih ali najemnih pogodbah. Verjetno bi se našlo še kaj, vendar najpogosteje gre za tovrstne osebne podatke.

Ali imate morda določene tudi zbirke osebnih podatkov?

Ne, formalno nimamo nič posebej določeno.

B2 Glede na to, da nimate določenih zbirk osebnih podatkov, kako potem zagotavljate pregled nad tem katere osebne podatke obdelujete in kako z njimi ravnate?

Posebnega sistema za pregled ali nadzor nad osebnimi podatki nimamo vzpostavljenega. Z njimi ravnamo skrbno in v okviru obstoječih delovnih procesov, ampak res pa nimamo nekih

ločenih evidenc ali posebnih postopkov, namenjenih posebej varstvu osebnih podatkov. Po mojem mnenju bi uvedba dodatnih sistemov ali evidenc pomenila predvsem dodatno administrativno obremenitev v časovni vložek, ki ga v praksi trenutno težko zagotovimo.

B3 Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Ne nimamo.

B4 Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate?

Ne, trenutno še nimamo.

B5 Ste že razmišljali o tem, da bi vzpostavili pravilnik oz. notranjo politiko o varstvu osebnih podatkov? Kateri so razlogi, da tega še niste storili?

O tem sem že razmišljala in imam namen, da bi to v prihodnje uredila. Se pa tega še nisem resno lotila in se tudi nisem podrobneje pozanimala, kaj vse bi bilo potrebno vključiti. Verjetno bi se najprej pozanimala kako imajo to urejeno v kakšnem drugem računovodskem servisu, da se lahko potem sama bolje lotim zadeve. V prvi vrsti bi predvsem rada uredila pogodbe s strankami.

Glavni razlog, da pravilnik še ne obstaja pa je predvsem pomanjkanje časa in dejstvo, da se v praksi najdejo bolj nujne naloge oz. dela, ki imajo prednost.

B6 Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja?

Zaposleni so s splošnimi načeli ravnanja seznanjeni preko vsakodnevnega dela in mojih ustnih navodil oz. usmeritev. Posebnih ali rednih usposabljanj na tem področju pa nimamo organiziranih. Ocenila, bi da je njihovo znanje dobro.

B7 Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)?

Na noben poseben oz. formalen način tega ne preverjamo. Načeloma zaposleni vedo, da morajo z vsemi podatki ravnati skrbno in zaupno. V računovodstvu so namreč praktično vsi podatki delikatne narave. Zato se mi zdi da osebni podatki v tem smislu niso neka posebna izjema, čeprav je res, da za zanje veljajo še določene dodatne zahteve in omejitve.

B8 Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?

Ne, posebnega protokola za takšne primere nimamo pripravljenega. Če bi prišlo do situacije, da bi recimo zaposleni pomotoma poslal napačen dokument, ki bi vseboval osebne podatke, napačni osebi, bi stranko o tem obvestili in se ji opravičili. Dodatnih formalnih postopkov pa zaenkrat nimamo dorečenih.

C1 Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov?

Trenutno tega področja še nimamo urejenega. Imamo pa vsekakor namen te pogodbe urediti. Kot sem že omenila prej, je to ena od stvari, ki jih želim spraviti v red, predvidoma drugo leto poleti, če bo šlo vse po načrtih in nas kaj ne preseneti.

Kaj pa je razlog, da nimate sklenjenih pogodb, če smem vprašati?

Razlog je enak kor pri pravilniku. Enostavno nam primanjkuje časa, da bi vse uredili. V praksi se namreč pogosto zgodi, da tudi kadar imamo namen to področje urediti, pridejo vmes druge bolj nujne zadeve, ki zahtevajo takojšnjo obravnavo in jim moramo dati prednost. Zaradi tekočega, sprotnega dela se te stvari posledično večkrat preložijo, čeprav se zavedam, da jih bo potrebno slej kot prej urediti.

C2 Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate?

Ne, tega ne vodimo.

C3 Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki?

Trenutno jih formalno nimamo določenih. V praksi pa večji del podatkov hranimo do zaključka bilanc, nato fizično dokumentacijo vrnemo strankam. Kar se tiče elektronskih podatkov, torej podatkov v programih in na samih računalnikih, pa so ti večinoma shranjeni trajno. Gre predvsem za pogodbe, oddane obračune DDV, podatke o plačah in tudi kakšne druge dokumente, ki nastajajo v okviru našega dela. Podatke praviloma brišemo šele, ko s stranko prekinemo poslovno sodelovanje.

C4 Kako pa se potem v praksi znajdete, ko pride do vprašanja, koliko časa je treba kakšne podatke hraniti?

Jah, tega področja trenutno nimamo urejenega. Mislim sicer, da v praksi ne delamo nič narobe, ampak se zavedam, da bi bilo bolj prav, če bi imeli roke jasno določene v kakšnem notranjem pravilniku ali podobnem dokumentu, ki bi nam služil kot jasna usmeritev.

D1 Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov?

Na splošno imamo vzpostavljene osnovne varnostne ukrepe za zaščito vseh podatkov. Na primer računalnike imamo zaščitene z gesli, poslovni prostori so zaklenjeni, dostop je mogoč le če obiskovalec pozvoni in mu odpremo. Potem izven delovnega časa so prostori dodatno zaščiteni tudi z alarmnim sistemom. Dokumentacijo, ki je povezana s plačami imamo shranjeno posebej v omarah, ki so zaklenjene, do njih pa imamo dostop le zaposleni, ki dejansko delamo na obračunih plač. Verjetno obstajajo še kakšni drugi ukrepi, ampak se jih v tem trenutku ne spomnim. V osnovi pa gre predvsem za te ukrepe.

D2 Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe?

To zagotavljamo predvsem z ukrepi, ki sem jih ravnokar omenila – torej zaščita računalnikov z gesli, zaklenjene pisarne, omare za dokumentacijo in še drugo.

D3 Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

Vzpostavljeno imamo šifrirano pošiljanje plačilnih list po elektronski pošti. Kar se tiče varnostnih kopij podatkov, jih seveda izvajamo ampak predvsem z vidika splošne varnosti in zaščite pred izgubo podatkov, na primer v primeru okvare računalnikov, udara strele ali podobnih nepredvidljivih dogodkov. Po navadi delam tedenske varnostne kopije na zunanji disk, po potrebi pa tudi pogosteje.

D4 Kje se ti podatki hranijo in kdo ima dostop do njih?

Varnostne kopije podatkov hranim v zaklenjeni omari v pisarni, do katere imam dostop samo jaz. V izrednih okoliščinah oz. v primeru večjih težav, kadar je potrebno ponovno vzpostaviti sistem, ima dostop do teh podatkov tudi naš računalničar.

E1 Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj?

Rakla bi, da s podatki ravnamo skrbno in odgovorno, ampak se pa hkrati tudi zavedam, da nimamo vsega formalno urejenega. Kot največjo pomanjkljivost vidim predvsem, da nimamo notranjega pravilnika in pogodbenih ureditev s strankami, kar bi si v prihodnje še želeli urediti.

E2 Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki?

Ne, do sedaj še niso imeli nobene revizije ali nadzora. Če i ga imeli, bi verjetno tudi že imeli urejeno vso potrebno dokumentacijo.

E3 Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)?

Torej če prav razumem vprašanje, gre na primer za situacijo ko zaposleni pri naši stranki stopi v stik z nami in želi informacije o svojih osebnih podatkih, njihov popravek ali izbris?

Ja, tako je

V takih primerih posameznika vedno usmerimo na njegovega delodajalca, torej na naš stranko. Z zaposlenimi naših strank neposredno nimamo komunikacije in jim ne posredujemo nobenih podatkov. Ko pa zahteva pride s stani naše stranke pa ji seveda ugodimo. Načeloma s tem nimamo večjih težav, saj so stranke navajene, da takšne zadeve rešujejo same. Se pa občasno zgodi, da kakšna stranka zaposlenega »pošlje« kar k nam v računovodstvo. V tem primeru ga preusmerimo nazaj k delodajalcu.

E4 Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

Enako kot sem že omenila. Posameznika bi prijazno obvestili, da mora zahtevo nasloviti na svojega delodajalca, saj imamo pogodbeno razmerje z njim.

E5 Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas, čeprav v praksi običajno nimate stika z njimi?

Ne, nekih formalnih, zapisanih postopkov za takšne primere nimamo. Imamo pa znotraj podjetja z zaposlenimi nek splošen dogovor o tem kako v takšnih situacijah ravnamo. Če se zgodi, da posameznik zahtevo naslovi neposredno na nas potem bodisi o tem obvestimo našo stranko ali pa posameznika usmerimo nazaj k njej. Namen tega je, da zahteva vedno pride do nas preko naše stranke.

F1 Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih?

Mislim, da je največji izziv predvsem to, da skladnost z zakonodajo zahteva precej časa, če želiš imeti vse urejeno kot je treba. Vzpostaviti je treba celoten sistem kot so notranji pravilnik, opredeliti zbirke osebnih podatkov, urediti pogodbe s strankami, poskrbeti za izobraževanje sebe in zaposlenih ter redno skrbeti za brisanje podatkov v skladu z določenimi roki. Vse to zahteva kar precej dodatne organizacije in dela. Pa tudi dodatni strošek ni zanemarljiv.

F2 Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate?

Ne, zaenkrat te dokumentacije še nimamo urejene. V bistvu nam trenutno še vse manjka. Planiram se tega lotiti, če bo vse po sreči, drugo leto poleti.

F3 Ali imate morda narejeno oceno učinkov tveganja za zlorabo osebnih podatkov?

Ne, nimamo.

F4 Če bi naredili oceno tveganja za zlorabo osebnih podatkov, kako bi ocenili, kje pri vas obstajajo največja tveganja in s kakšnimi vrstami tveganj se sploh soočate?

Načeloma mislim, da nekih res hudih tveganj pri nas ni, saj poslujemo dokaj previdno. Kljub temu pa seveda vedno obstajajo določena tveganja. To so na primer možnost vdora v računalnike, fizični vdor v pisarne, pa tudi višja sila kot sta požar, poplava in podobno. Poleg tega obstaja tveganje nepooblaščenega dostopa do podatkov ali pa človeške napake, na primer, da se pošlje napačne podatke napačni osebi.

G1 Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela?

Zaenkrat zakonodaja na naše vsakodnevno delo in organizacijo ni bistveno vplivala. Večjih sprememb v praksi še nismo uvajali.

G2 Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Ne, zaenkrat še nismo uvedli nobenih novih storitev, postopkov ali tehnologij izključno zaradi varstva osebnih podatkov. Trenutno smo v fazi, kjer se zavedamo, da je najprej treba urediti vso potrebno dokumentacijo na tem področju. Šele potem bomo lahko razmišljali naprej tudi o morebitnih nadaljnjih korakih.

Priloga 8: Transkript intervjuja INT5

A1 Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih?

Rekla bi, da jih poznam kar dobro. Seveda bi jih lahko poznala še bolje, ker se zakonodaja vendarle spreminja, ampak mislim, da osnovne zahteve poznam. Zavedam se, kaj se od računovodskega servisa pričakuje in kje so glavna tveganja. Verjetno pa kakšno dodatno izobraževanje na to temo zagotovo ne bi škodilo.

A2 Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?

Po mojem mnenji je ključno predvsem to, da ne prihaja do neupravičenih razkritij osebnih podatkov. To pomeni varno hranjenje in nadzor nad tem, da do podatkov nima dostopa vsak, ampak samo pooblaščeni zaposleni. Prav tako se mi zdi zelo pomembno, da so vsi, ki delajo s temi podatki seznanjeni z osnovnimi pravili in se zavedajo, da gre za občutljive informacije, s katerimi je treba ravnati previdno.

B1 Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov?

Zbirk osebnih podatkov sicer nimam določenih, je pa osebnih podatkov v računovodstvu kar nekaj. Največ jih je povezanih z obračunom plač in s pogodbami. Najpogosteje gre za ime, priimek, naslov, elektronski naslov, davčno številko, EMŠO in podobne podatke. Drugega osebno mislim, da ni prav veliko. Vsaj ne v takšnem obsegu kot pri plačah. Se pa osebni podatki pojavljajo tudi v kakšnih drugih dokumentih, ne samo pri plačah. Recimo kakšne pogodbe, računi, včasih dobim tudi kakšno kopijo osebnega dokumenta, ki jo potem takoj po vnosu podatkov v bazo izbrišem in podobno.

B2 Glede na to, da nimate določenih zbirk osebnih podatkov, kako potem zagotavljate pregled nad tem katere osebne podatke obdelujete in kako z njimi ravnate?

Če sem povsem iskrena nekega organiziranega pregleda nimam. Vem s kakšnimi podatki delam oz. delamo, ker gre za vsakodnevno delo, nimam pa tega izoblikovanega v nekih evidencah ali preglednih seznamih.

B3 Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Ne, nimamo.

B4 Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate?

Ne, tudi tega nimamo.

B5 Ste že razmišljali o tem, da bi vzpostavili pravilnik oz. notranjo politiko o varstvu osebnih podatkov? Kateri so razlogi, da tega še niste storili?

Ja, zavedam se, da bi bilo prav, da bi se to uredilo in da bi bilo smiselno imeti tak pravilnik, ampak realno gledano gre za kar obsežen projekt o katerem čisto iskreno povedano še nisem resno razmišljala.

Kateri so razlogi, da tega še niste storili? Kaj bi vas spodbudilo, da bi ga uvedli?

Če povem po pravici, gre tukaj predvsem za dodaten strošek in dodatno delo. Kadar gre za neko novost, ko mi dolgoročno olajša delo ali mi zmanjša obseg dela, sem takoj za. V tem primeru pa gre sicer za zakonsko obveznost, ampak konkretnih koristi pri vsakodnevnem delu nimam. Gre predvsem za dodatno dokumentacijo in papirologijo. Poleg tega pa ne pomeni samo uvedbe pravilnika znotraj podjetja ampak je treba vse skupaj pogodbeno urediti tudi s strankami, kar pa še dodatno poveča obseg dodatnega dela.

B6 Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja?

Ne, posebnih usposabljanj, ki bi bila namenjena izključno varstvu osebnih podatkov nimam. Sva samo dve zaposleni. Jaz imam čez vso komunikacijo s strankami in tudi obračune plač, sodelavka pa se ukvarja predvsem s knjiženjem. Ne morem sicer reči, da se z osebnimi podatki nikoli ne sreča, ampak ni neke večje nevarnosti, da bi z njimi ravnala neustrezno. Z njimi ravna skrbno, tako kot z vsemi ostalimi podatki s katerimi delamo v računovodstvu.

B7 Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)?

Na to bom odgovorila bolj splošno, ker nimam posebnih postopkov samo za varstvo osebnih podatkov. Gre bolj za splošen pristop k varovanju vseh podatkov v računovodstvu. Predvsem gre za opozorila in sprotno komunikacijo – če je kje potrebna večja previdnost, to potem poudarim. Do kakršnih koli sankcij ali kazni pa do zdaj še ni prišlo.

B8 Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?

Posebnega protokola za obveščanje v takih primerih nimam. Kot sem že omenila, imam komunikacijo s strankami v celoti čez jaz, prav z namenom, da se takšne napake ne bi dogajale. Še posebej pazim pri obračunih plač, ki so občutljivi z več vidikov. Ne spomnim se, da se bi mi kdaj zgodilo, da bi dokument poslala napačni osebi. Če pa bi do česa takega prišlo, bi o tem najprej obvestila stranko, ki je bila s tem prizadeta.

C1 Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov?

Ne nimam nič.

Kaj pa je razlog, da nimate sklenjenih pogodb, če smem vprašati?

Razlog je v bistvu enak kot pri notranjem pravilniku. Po pravici povedano gre za dodaten strošek in dodatno delo. Če bi šlo za neko obveznost ali projekt, ki mi dolgoročno olajša delo ali zmanjša obseg vsakodnevnih opravil, sem takoj za. V tem primeru pa ne vidim neke dodane vrednosti.

C2 Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate?

Ne, je ne vodimo in posledično tudi ne posodabljam.

C3 Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki?

Rokov hrambe v smisli, da bi bili posebej določeni in zapisani, nimam. V praksi večino fizične dokumentacije po zaključenih bilancah vrnemo strankam. Pri podatkih o plačah pa je situacija nekoliko drugačna. Te podatke imamo shranjene, ker se pogosto zgodi, da stranke potrebujejo dostop do podatkov o plačah iz preteklih let in se v takšnih primerih vedno obrnejo na nas. Tudi takrat, ko imajo same vso dokumentacijo shranjeno v fizični obliki, pogosto pokličejo nas.

C4 Kako pa se potem v praksi znajdete, ko pride do vprašanja, koliko časa je treba kakšne podatke hraniti?

Če sem povsem iskrena, ne poznam natančnih rokov hrambe, kot jih določa zakonodaja o varstvu osebnih podatkov. Držim se rokov, ki veljajo po pravilih in zakonih na področju računovodstva. Tako se na primer podatki o plačah hranijo trajno oz. vsaj do prekinitve sodelovanja s stranko. Ostalo dokumentacijo pa, kot sem že omenila, vsako leto vrnem strankam, ki so potem samo odgovorne za nadaljnjo hrambo.

D1 Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov?

Če govorimo izključno o osebnih podatkih, specifičnih ukrepov prav za to nimamo.

Kaj pa na splošno ste zagotovili kakšne ukrepe za varnost podatkov? Na primer gesla na računalnikih, zaklepanje omar, pisarne in podobno?

Na splošno pa seveda imam uvedene osnovne ukrepe za varnost podatkov. Računalniki so zaščiteni z gesli, računovodski programi prav tako, še dodatno. Za določene stranke gesla v

programe poznam samo jaz. Pisarno imam zaklenjeno in pod alarmom in vhod v pisarno pod kamero.

D2 Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe?

Posebnih zapisanih postopkov nimam. Večina osebnih podatkov tako ali tako pride izključno do mene, sodelavka pa z njimi nima veliko stika. Tudi če se z njimi kdaj sreča, ji zaupam, da z njimi ravna ustrezno in odgovorno, tako da ne vidim nevarnosti.

Največjo pozornost namenjam temu, da se osebni podatki ne pošiljajo napačnim osebam in da do njih ne pridejo zunanji, nepooblaščeni posamezniki. To zagotovim s prej omenjenimi ukrepi. Pa tudi na primer, da občutljive dokumentacije ne puščam na vidnih mestih, plačilnih list fizično natisnjenih nimam razstavljenih na mizi, ampak jih pospravim v fascikel ali vsaj obrnem tako, da je na vrhu prazna stran.

D3 in D4 Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

Dvofaktorskih prijav nimamo. Plačilne liste pa po mailu pošiljamo šifrirano. Kar se tiče varnostnih kopij oz. backupov vseh podatkov, se ti izvajajo dnevno. Za to skrbi zunanji računalničar, sama se na tehnične podrobnosti ne spoznam. Vem pa, da ko se je v preteklosti nekaj od računalniške opreme pokvarilo, je obstajala varnostna kopija iz prejšnjega dne in je računalničar podatke brez težav vzpostavil nazaj, tako da praktično ni bilo izgube. Podatki se hranijo na strežniku, do katerega imava dostop jaz in računalničar. Poleg tega imam do določenih map, na primer map s plačami ali map s podatki določenih strank, dostop samo jaz s svojega računalnika. Sodelavka do teh map nima dostopa.

E1 Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj?

Verjetno ne morem reči, da smo popolnoma skladni. Predvsem zato, ker nimamo urejenih pravilnikov, pogodb, zbirk in ostalega. Po drugi strani pa mislim, da pri svojem delu zakonodaje dejansko ne kršimo. Z osebnimi podatki ravnamo previdno in odgovorno, tako, da bi rekla, da praksa v večji meri urejena, manjka nam pa še formalni del.

E2 Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki?

Ne, nadzora s tega področja še nismo imeli.

E3 Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)?

Nisem imela še nikoli takšnega primera.

A tudi stranka vas nikoli ni prosila za popravek naslova prebivališča ali TRR–ja pri zaposlenem recimo?

Aja, nisem prav razumela. To pa se seveda redno dogaja. V takih primerih pa seveda brez težav popravim.

E4 Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

Mislite na posameznika kot našo stranka ali kot recimo zaposlenega pri stranki?

Lahko poveste za oba primera če se razlikujeta.

Kadar zahtevo poda stranka potem ni nobenih težav – zahtevo izpolnimo. Če bi šlo pa za zaposlenega pri naši stranki, potem praviloma najprej stopim v stik s stranko in preverim oz. pridobim dovoljenje za spremembo ali posredovanje podatkov. Dokumentacijo tudi raje posredujem stranki in ne neposredno njihovemu zaposlenemu. Tako ravnam v večini primerov, ampak priznam, da kdaj ugodim tudi kakšnemu posamezniku, če vem da lahko.

Kaj pa recimo pravica do izbrisa? Če bi stranka ali zaposleni pri stranki zahteval izbris določenih podatkov?

Takega primera pa še nisem imela. Iskreno povedano si težko predstavljam, katere osebne podatke bi sploh lahko izbrisali, saj smo pri določenih podatkih zakonsko vezani, da jih hranimo. Plače recimo. Če bi se znašla v takšni situaciji, bi se verjetno s kom posvetovala. Ali s kolegi iz drugih računovodstev ali pa z odvetnikom navsezadnje.

E5 Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas, čeprav v praksi običajno nimate stika z njimi?

Ne, nimamo nobenih postopkov. Ravnala bi tako kot sem prej omenila. Zahtevo bi po navadi najprej preverila pri stranki.

F1 Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih?

Rekla bi, da sta največja izziva predvsem pomanjkanje časa in pa tudi znanja na tem področju, da bi se sama lotila priprave pravne podlage, kar pomeni, da bi za to morala najeti nekoga zunanjega in to pomeni potem tudi dodaten strošek.

F2 Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate?

Ne, nimam praktično nobene dokumentacije. Po pravici povedano, niti ne vem kaj vse bi morala imeti. Vem za notranji pravilnik in pogodbe s strankami.

F3 Ali imate morda narejeno oceno učinkov tveganja za zlorabo osebnih podatkov?

Ne, kot sem rekla nimam ničesar.

F4 Če bi naredili oceno tveganja za zlorabo osebnih podatkov, kako bi ocenili, kje pri vas obstajajo največja tveganja in s kakšnimi vrstami tveganj se sploh soočate?

Vedno obstaja neko tveganje, na primer da pride do vloma v pisarno ali do kakšne nesreče pri kateri se izgubijo podatki – na primer se pokvari računalnik zaradi udara strele. Ne bi pa rekla, da smo bolj izpostavljeni kot so druga računovodstva. Takšna tveganja pač obstajajo povsod. Po mojem mnenju je največje tveganje za zlorabo osebnih podatkov naša napaka. Pomotoma razkriješ podatke osebi, ki jih ne bi smel. Ampak tega se zelo zavedam in sem res pazljiva in dosledna.

G1 Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela?

Zakonodaja na naše delovne procese in organizacijo ni imela vpliva, saj zaradi nje nismo uvajali nobenih posebnih sprememb. Že prej smo z vsemi podatki, med drugim tudi z osebnimi ravnali previdno.

G2 Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Ne, nismo uvedli nič na novo.

Priloga 9: Transkript intervjuja INT6

A1 Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih?

Recimo nekje srednje dobro. Zakonov priznam, da nisem brala, tako da vsega ne vem, ampak osnove za delo v računovodstvu pa poznam.

A2 Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?

Rekla bi, da je pomembno, da so podatki dobro zavarovani, da do njih ne more kar vsak in pa da tisti, zaposleni, ki se z njimi srečujejo vedo, da jih ne morejo kar pošiljati na okoli vsepovprek ampak potrebujejo za to neko upravičeno podlago.

B1 Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov?

Osebnih podatkov glede na celoto podatkov, ki jih pridobimo, bi rekla da ni spet toliko. Predvsem gre za podatke pri plačah, podjemnih pogodbah, avtorskih honorarjih, najemninah in podobnem.

Za kakšne osebne podatke pa gre to? Ime, priimek..?

Ja, ime, priimek, naslov, davčna številka, EMŠO in podobno. Kakšna telefonska številka včasih, mail, tudi TRR seveda.

Ali imate določene zbirke osebnih podatkov?

Ne, nimamo določenih.

B2 Glede na to, da nimate določenih zbirk osebnih podatkov, kako potem zagotavljate pregled nad tem katere osebne podatke obdelujete in kako z njimi ravnate?

Na to se po pravici povedano niti ne osredotočamo. Načeloma se srečujemo z osebnimi podatki bolj ali manj pri plačah, ki pa so v vsakem primeru delikatna zadeva in tam ravnamo še posebej pazljivo. Nimamo pa nekega posebnega sistema.

B3 Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Ne, nimamo.

B4 Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate?

Ne, nimamo.

B5 Ste že razmišljali o tem, da bi vzpostavili pravilnik oz. notranjo politiko o varstvu osebnih podatkov? Kateri so razlogi, da tega še niste storili?

Vem, da bi načeloma to po zakonu morali imeti, ampak še nimamo. Konkretno nisem še razmišljala o tem, da bi se lotila priprave vsega kar je s tega področja predpisano, ampak bo slej kot prej prišlo tudi to na vrsto. Navsezadnje je to le neka formalna zadeva. Vedno damo nekako prednost stvarem, ki so v tistem trenutku bolj nujne. Pa ne govorim samo o področju varstva osebnih podatkov ampak tudi o drugih področjih. Je en kup pravilnikov, ki jih je treba imeti. Vsako leto je kakšen nov, potem je treba tiste, ki jih že imaš obnavljati, je en kup »papirjev«. Vsakih nekaj let se potem lotim in obnovim tiste, ki jih že imam in dam narediti še nove. Tako, da slej kot prej bomo uredili tudi to.

B6 Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja?

Ne, na tem področju nimamo usposabljanj, ampak bi rekla, da zaposleni kar dobro poznajo okvirje tega področja. Imamo davčna in računovodska usposabljanja, glede varstva osebnih podatkov pa ne. Če bi se recimo kaj konkretno spremenilo, kar bi imelo velik vpliv na naše delo bi se verjetno o tem izobrazila jaz potem pa bi pomembne spremembe predala naprej zaposlenim. Tako po navadi delamo tudi za druga izobraževanja, ker je za manjše podjetje predrago, da bi vsi hodili na vsa izobraževanja. Razen kadar gre za video–izobraževanja. Potem takrat pa poskusim vsem omogočit, da ga poslušajo.

B7 Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)?

Ne, nič tako dramatičnega. Nobenih testov ne dajemo za pisat. Lahko bi rekli spodbuda, opozorila, če bi bila potreba potem kazen ampak do zdaj res še nismo imeli take situacije. Tako kot sem omenila, jaz jih opozorim oz. jim povem na kaj morajo biti pozorni in sodelavci to upoštevajo.

B8 Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?

Ne, informacijskega pooblaščenca ne bi obveščali, tudi protokola nimamo. Če bi šlo za neko kršitev bi o tem obvestili stranko, da potem lahko ustrezno ukrepa naprej.

C1 Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov?

Ne, nimamo.

Kaj pa je razlog, da nimate sklenjenih pogodb, če smem vprašati?

Zato, ker je to precej zamudno in žal še ni prišlo na vrsto. Verjetno bomo istočasno, ko bomo urejali pravilnike, uredili še pogodbe.

C2 Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate?

Ne ne vodimo je.

C3 Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki?

Rokov hrambe nimamo določenih. V bistvu se držimo rokov, ki so na splošno določeni v računovodstvu.

Koliko časa pa potem recimo hranite določene podatke?

Načeloma kar je v fizični obliki vračamo strankam na tam nekje 2–3 leta. Kar je pa shranjeno v programih, na mreži in v oblaku – torej google drive–u, kamor stranke nalagajo dokumentacijo pa načeloma ne brišemo. Brisali bi recimo v primeru ko določene stranke nimamo več. Takrat oni recimo odstranijo naše dostope do datotek v oblaku, mi pa po predaji dokumentacije pobrišemo zadeve v programih in na mreži.

C4 Kako pa se potem v praksi znajdete, ko pride do vprašanja, koliko časa je treba kakšne podatke hraniti?

Priznam, da glede osebnih podatkov okoli hrambe ne vem natančno rokov, ampak glede na to, da se osebni podatki pri nas pojavljajo večinoma pri obračunih plač, ki jih je treba hraniti trajno, mislim, da to zadevo nekoliko olajša.

D1 Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov?

Zaradi osebnih podatkov nismo uvedli nič. Imamo pa na splošno poskrbljeno za varnost vseh podatkov.

Katere ukrepe pa ste uvedli za varstvo podatkov na splošno?

To pa prakticiramo že dalj časa, ni nič na novo, ampak fizične podatke varujemo tako, da imamo čim boljši nadzor nad tem kdo pride v poslovne prostore – torej da jih zaklepamo, imamo alarm, vezan na varnostno službo, kamero pred vhodom in pa odklepanje pisarn s kodo ali kartico – da vemo točno kdo od zaposlenih je kdaj vstopil – to služi tudi kot »štempljanje«. Potem elektronske podatke pa imamo zaščitene z gesli večinoma, morda se sem lahko štejejo tudi antivirusni programi.

D2 Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe?

Z vsem kar sem ravnokar naštela. Predvsem bi pa poudarila, da je potrebno imeti sodelavce oz. zaposlene, ki jim lahko zaupaš, da informacij ne bodo raznašali izven službe. To pač pokaže čas, dostop do informacij in podatkov pa jim »širiš postopoma«, ko zaupanje raste.

D3 Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

Dvofaktorsko prijavo imamo v bankah če se ne motim – imamo dostop do spletnih bank strank, da v njihovem imenu plačujemo in svoje banke. Potem vem, da so plačilne liste, ki jih pošljemo po mailu šifrirane, avtorske pogodbe, podjemne, občasno delo itd. Varnostne kopije izvajamo redno, mislim, da se samodejno izvajajo dnevno, ponoči enkrat.

D4 Kje pa se ti podatki hranijo in kdo ima dostop do njih?

Hranijo se v naših poslovnih prostorih oz. mislim, da celo v neke vrste oblaku, nisem prepričana. Dostop do njih ima naše IT podjetje, ki skrbi za vzdrževanje, torej njihovi zaposleni. Jaz načeloma imam dostop, ampak mi ne koristi, ker teh podatkov ne znam narediti uporabnih. Je pa narejena dnevno kopija tako, da če pride do kakšnega izpada in bi se podatki uničili – obstaja kopija, ker se v kratkem času lahko vse vzpostavi nazaj.

E1 Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj?

Mislim, da skladni z zakonodajo nismo povsem. S podatki bi rekla, da ravnamo odgovorno in previdno. Zagotovo pa nimamo določenih rokov hrambe, evidenc obdelave, zbirk podatkov, pogodb s poslovnimi partnerji, potem ne izobražujemo se dovolj na tem področju.

E2 Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki?

Ne, nismo še imeli.

E3 Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)?

Če posameznik želi dostopati do svojih osebnih podatkov, ali recimo želi, da jih popravimo ali celo jih izbrišemo, to storimo. Razen, če jih recimo zakonsko ne bi smeli izbrisati. Ampak takega primera še nismo imeli, tudi nobene zahteve za dostop do podatkov nismo imeli. Še najbolj bi rekla, da prošnja ali morda bi temu rekla obvestilo o popravku osebnih podatkov. Recimo, da kdo želi, da se mu pošilja plačilna lista na drug e–mail naslov.

E4 Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

Zahtevi za izbris bi ugodili, če bi bila pravno utemeljena. Mi podatkov ne moramo kar brisati. Po navadi delamo z osebnimi podatki oz. jih pridobimo samo kadar res moramo. Osebne podatke potrebujemo pri obračunu plač in za to obstaja zakonska obveza, torej jih ne moremo kar izbrisati na željo posameznika. Če pa bi imeli primer, ko bi neustrezno oz. neutemeljeno hranili osebne podatke posameznika pa bi jih izbrisali. Zahtevi za popravek in dostop pa bi ugodili.

E5 Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas?

Ne, nimamo nobenih postopkov.

F1 Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih?

Rekla bi, da predvsem, izzivi, ki jih še nismo odpravili – torej tista področja kjer še nismo skladni z zakonodajo.

F2 Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate?

Ne, v bistvu od dokumentacije nimamo praktično še nič urejenega.

F3 Ali imate morda narejeno oceno učinkov tveganja za zlorabo osebnih podatkov?

Ne, nimamo

F4 Če bi naredili oceno tveganja za zlorabo osebnih podatkov, kako bi ocenili, kje pri vas obstajajo največja tveganja in s kakšnimi vrstami tveganj se sploh soočate?

Načeloma mislim, da nekih pretiranih tveganj ni. Tudi v primeru izgube podatkov zaradi neke višje sile, vdora, kraje recimo, imamo poskrbljeno z varnostnimi kopijami. Tudi prostori so fizično zavarovani kolikor je možno. Mogoče je še največja »nevarnost«, da recimo pošlješ sporočilo z osebnimi ali pa že samo z občutljivimi podatki, napačni osebi.

G1 Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela?

Ne morem reči, da je imela nek velik vpliv zaenkrat.

G2 Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Zaradi GDPR–ja in ZVOP–2 konkretno nismo uvedli nobene novosti. Mislim, da imamo v sklopu »varovanja« vseh podatkov dosežen zadovoljiv nivo varnosti.

Priloga 10: Transkript intervjuja INT7

A1 Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih?

Rekla bi, da imam osnovno znanje, ampak daleč od tega, da bi poznala vse podrobnosti. Vsekakor bi lahko znanje še nadgradila.

A2 Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?

Najpomembnejše se mi zdi, da so osebni podatki na varnem in da do njih nimajo dostopa vsi, ampak samo tisti, ki z njimi znajo pravilno ravnati. Z vidika zakonodaje pa se mi zdi pomembno tudi, da ima podjetje urejeno vso predpisano dokumentacijo.

B1 Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov?

Pridobivamo veliko podatkov na sploh, ampak glede osebnih pa ne bi rekla, da jih prav veliko. Predvsem pri obračunih plač in raznih pogodb o delu. Tam se zbirajo ime, priimek, naslov, davčna številka, elektronski naslov in še kaj verjetno. Potem vem, da za eno podjetje izdajamo račune in izdamo veliko fizičnim osebam, kjer spet zberemo ime, priimek, naslov bivanja in elektronski naslov.

Zbirk osebnih podatkov pa nimamo določenih.

B2 Glede na to, da nimate določenih zbirk osebnih podatkov, kako potem zagotavljate pregled nad tem katere osebne podatke obdelujete in kako z njimi ravnate?

Nimamo nekega metodičnega pregleda..

B3 Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Ne, nimamo.

B4 Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate?

Ne nimamo.

B5 Ste že razmišljali o tem, da bi vzpostavili pravilnik oz. notranjo politiko o varstvu osebnih podatkov? Kateri so razlogi, da tega še niste storili?

Ja, sem, ampak ni bilo še časa se bolj resno posvetiti temu. Najprej imamo v planu še uvesti nekaj novosti. Razmišljamo tudi o zamenjavi programov, ker imamo z obstoječimi kar nekaj težav. Tako da ima to vse definitivno prednost. Računam, da bomo v roku leta do dveh našli čas, da uredimo še to.

Mislim pa, da lahko vzorce vseh potrebnih dokumentov kupiš tudi preko zbornice računovodskih servisov, sem enkrat slučajno videla. Ampak bi bilo potrebno preveriti ali se bolj splača to, ali da ti vse skupaj pripravi pravnik. Mislim, da je vseeno lažje če ti vse skupaj pripravi pravnik, pa tudi morda si bolj siguren, da imaš vse urejeno, kot je potrebno prav za tvoje podjetje. Sploh če si tako kot jaz in se ne spoznaš na to področje. In vseeno nekdo potem stoji za tem kar je pripravil.

B6 Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja?

Ne izvajamo nobenega usposabljanja. Potrudim se, da jih seznanim z vsemi novostmi, ki se dogajajo. Zaposleni tudi hodijo na izobraževanja, ampak so ta po navadi bolj usmerjena v samo računovodstvo. Kar se tiče pa varstva osebnih podatkov pa imamo nekoliko bolj po domače, če lahko tako rečem. Imajo pa zaposleni tudi vedno dostop do vseh novičk, ki jih prejmemo preko e pošte in pa do revij na katere smo naročeni.

B7 Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)?

Jih ne preverjam. Če bi prišlo do kakšne napake bi jih seveda opozorila. Ampak načeloma res nimamo takšnih primerov. Da bi pa prav preverjala s kakšnimi kvizi ali podobno pa ne preverjam.

B8 Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?

Nimamo nobenega protokola. Do zdaj nekih resnih primerov kršitev nismo imeli. Se pa seveda kdaj zgodi, da komu kaj narobe pošlješ. Lahko, da so bili vmes tudi kakšni nepravilno poslani osebni podatki. V primeru, ko pa pride do kakšnih kršitev, bi bilo prav, da obvestimo tako stranko, ki je bila oškodovana, kot tudi informacijskega pooblaščenca. V praksi je tako, da če že obvestimo stranko, informacijskega pooblaščenca sploh ne. Ampak tudi stranke najbrž ne bi obvestili, če bi šlo za neko manjšo kršitev, ker bi verjetno začeli komplicirati. Vem, da ni ravno čisto prav ampak če povem po pravici je tako. Ampak res načeloma do takih stvari ne prihaja, ker tako jaz kot tudi vsi zaposleni res pazimo.

C1 Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov?

Ne, nimamo še.

Kaj pa je razlog, da nimate sklenjenih pogodb, če smem vprašati?

Težko rečem. Morda to, da se mi ne zdi to prioriteta. So mi pomembnejše kakšne druge stvari. Saj vem da ni prav, ampak tako je. Pa že kakšnim pomembnejšim stvarem včasih ne morem posvetiti dovolj časa. Recimo menjavi programov. Se lotevamo že nekaj časa pa se še kar vleče.

C2 Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate?

Ne, ne vodimo.

C3 Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki?

Ne določamo in ne nadzorujemo. Glede rokov hrambe, se držimo predvsem računovodskih predpisov. Večino dokumentacije pa tako ali tako vrnemo najkasneje do maja meseca ko se zadeve po bilancah in aprilskem obračunu DDV–jev malo umirijo.

C4 Kako pa se potem v praksi znajdete, ko pride do vprašanja, koliko časa je treba kakšne podatke hraniti?

Kot sem že povedala nekega posebnega poudarka temu ne dajemo, verjetno tudi delamo kje kakšne napake, ampak tu se bolj fokusiramo na računovodske predpise. Dokumentacijo pa tako ali tako vračamo, kar hranimo od dokumentacije je le v elektronski obliki in kar ostaja shranjeno v programih. So to recimo tudi obračuni plač, ampak v skladu z računovodskimi predpisi je to potrebno hraniti trajno.

D1 Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov?

Nobenih.

Kaj pa na sploh? Kakšna gesla na računalnikih, zaklepanje pisarn?

Ja, to pa seveda. Za podatke na sploh, kar verjamem, da »koristi« tudi osebnim podatkom pa imamo antivirusne programe, gesla na računalnikih, poslovni prostori so zaklenjeni, tako, da morajo stranke pozvoniti in jim mi odpremo preko domofona.

D2 Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe?

Tako, da so poslovni prostori vedno zaklenjeni, da imamo nadzor nad tem kdo pride v njih. Na računalnikih so gesla, tako da ne more vsak dostopati do podatkov. Od zaposlenih pa imamo vsi dostop. Razen recimo, če bi prišel kakšen dijak ali študent na prakso, bi ga dali

na računalnik, ki nima dostopa do vseh podatkov – gesla na drugih računalnikih pa so tako ali tako različna.

D3 Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

Plačilne liste po mailu vem da pošiljamo šifrirano. Kaj pa mislite z rednim varnostnim kopiranjem podatkov?

D4 Če imate kakšne varnostne kopije, da v primeru kakšne nesreče ne izgubite vseh podatkov?

Ja, imamo, ampak ne specifično za osebne podatke.

Kje se ti podatki hranijo in kdo ima dostop do njih?

Dostop do njih imajo računalničarji, hrani pa mislim, da se pri nas v pisarni.

E1 Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj?

Nismo najbolj skladni. S podatki drugače delamo previdno, ampak res pa je, da nam ne bi škodilo kakšno izobraževanje iz tega področja. Prav tako pa nimamo sprejetega pravilnika, določenih rokov hrambe, zbirk osebnih podatkov, pogodb s strankami in verjetno še česa.

E2 Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki?

Ne nismo.

E3 Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)?

Nismo še nikoli obravnavali. Vsaj ne tako formalno. Če pa posameznik zahteva popravek svojih osebnih podatkov pa jih seveda popravimo.

E4 Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

Kar se tiče pravice do dostopa, načeloma ne zbiramo zdaj nekih strašnih osebnih podatkov, tako da ne vem kakšen smisel ima, da jih zahtevajo, ampak v tem primeru bi jih posredovali. Čeprav gre za ime priimek, naslov, davčno, EMŠO, TRR in elektronski naslov. Več skoraj ne. Glede pravice do popravka, ni nobenega dvoma. Seveda bi popravili, saj smo tudi dolžni popraviti, če se recimo nekdo preseli in zamenja svoj naslov ali kaj drugega. Pri pravici do

izbrisa pa iskreno ne vem. Osebnih podatkov posameznika mi ne smemo brisati, ker jih rabimo za obračun plače, tako da v tem primeru te pravice ne bi mogli izpolniti.

E5 Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas?

Ne nimamo.

F1 Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih?

Težko rečem, da sploh zagotavljamo neko skladnost, ker veliko stvari še nimamo povsem dodelanih. Ampak na splošno bi rekla, da predvsem čas, ki ga moraš nameniti, da vse urediš. Mi se ravno zato tega še nismo lotili.

F2 Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate?

Nimamo nič v bistvu.

F3 Ali imate morda narejeno oceno učinkov tveganja za zlorabo osebnih podatkov?

Ne, nimamo

F4 Če bi naredili oceno tveganja za zlorabo osebnih podatkov, kako bi ocenili, kje pri vas obstajajo največja tveganja in s kakšnimi vrstami tveganj se sploh soočate?

Po mojem to, o čemer sva govorili prej. Da po pomoti pošlješ osebne podatke nekoga, napačni osebi.

G1 Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela?

Ne bi rekla, da je sploh vplivala še zaenkrat.

G2 Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Ne, nismo.

Priloga 11: Transkript intervjuja INT8

A1 Kako dobro ocenjujete, da poznate zahteve Splošne uredbe o varstvu osebnih podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP–2), ki se nanašajo na delo v računovodskih servisih?

Mislim, da dobro.

A2 Katere ključne obveznosti glede varstva osebnih podatkov po vašem mnenju zadevajo računovodske servise?

Varno in odgovorno ravnanje z njimi. Poskrbeti je potrebno, da zaposleni odgovorno ravnajo z njimi, da ne pride do neželenih razkritji. Osebni podatki morajo biti varno shranjeni, vpogleda pa ne sme imeti vsak. Samo pooblaščene osebe, ki so odgovorne in vedo kako pravilno ravnati z osebnimi podatki.

B1 Katere osebne podatke v vašem računovodskem servisu po vašem mnenju pridobivate? Ali imate določene zbirke osebnih podatkov?

Prav posebnih zbirk nimamo določenih, večinoma pa so podatki, ki jih pridobivamo recimo ime, priimek, naslov, EMŠO, davčna številka, email, telefonska številka in podobno. Pridobimo drugače ogromno enih podatkov, ampak osebnih je od tega nek manjši del od celote.

B2 Glede na to, da nimate določenih zbirk osebnih podatkov, kako potem zagotavljate pregled nad tem katere osebne podatke obdelujete in kako z njimi ravnate?

Nimamo nekega posebnega pregleda in nadzora nad osebnimi podatki. Vemo kateri podatki so pač osebni in temu primerno z njimi ravnamo. Se pa recimo bolj pojavljajo osebni podatki pri obračunih plač, kjer pa imamo pregled in sistem obdelave določen interno, ustno v podjetju. Na splošno so plače bolj delikatne, tako da smo pri njih še posebej pazljivi in natančni.

B3 Imate v računovodskem servisu imenovano osebo, ki je odgovorna za varstvo osebnih podatkov?

Ne, nimamo.

B4 Ali imate vzpostavljeno notranjo politiko oz. pravilnik o varstvu osebnih podatkov? Če ga imate, kako pogosto ga posodabljate?

Ne, nimamo.

B5 Ste že razmišljali o tem, da bi vzpostavili pravilnik oz. notranjo politiko o varstvu osebnih podatkov? Kateri so razlogi, da tega še niste storili?

Ne, o tem nisem še konkretno razmišljala. Ker mi to enostavno ni tako pomembno, je le neka formalnost, ki nič ne vpliva na naše delo.

B6 Kako so zaposleni seznanjeni z vašimi postopki glede varstva osebnih podatkov? Ali se izvajajo redna usposabljanja?

Redno se usposabljamo bolj na tistih nujnih področjih za naše delo, imamo pa dostop do spletnih strani s članki in novostmi, tako da dostop do informacij imamo. Na področju varstva osebnih podatkov se ne izobražujemo tako zelo aktivno, spremljamo pa novosti.

B7 Kako preverjate in spodbujate zaposlene, da znajo ravnati v skladu s pravilnikom o varstvu osebnih podatkov – na primer z izvedbo testov, kvizov ali praktičnih primerov ter z različnimi oblikami motivacije (spodbude, opozorila, kazni..)?

Predvsem bi rekla, da z neko odprto komunikacijo in zaupanjem v zaposlene. Če imajo kakšno vprašanje me brez zadržka vprašajo, jaz jih seveda opozorim, če je kakšna novost ali morda nepravilnost. Ni pa nekega sistema kot je recimo reševanje testov.

B8 Ali imate pripravljen morda kakšen protokol za obveščanje strank in Informacijskega pooblaščenca v primeru kršitve varstva osebnih podatkov? Kako bi ukrepali, če bi zaposleni pomotoma poslal napačen dokument napačni osebni?

Rekli bi lahko, da imamo interni protokol, ki je nekako ustno dogovorjen, da se poslovnega partnerja o tem obvesti. Namerno tega zagotovo nobena sodelavka ne bi naredila, se pa kdaj seveda pomotoma tudi zgodi.

C1 Ali imate z naročniki (upravljalci podatkov) sklenjene pogodbe o obdelavi osebnih podatkov?

Ne, nimamo pogodb.

Kaj pa je razlog, da nimate sklenjenih pogodb, če smem vprašati?

Nisem še resno razmišljala o tem, da bi se lotila urejanja področja o varstvu osebnih podatkov. Prav bi bilo, da bi imeli to urejeno ampak se mi ne zdi tako pomembno za samo naše delo. Je samo neka formalnost. Saj verjetno bomo s časoma tudi to uredili.

C2 Ali vodite evidenco dejavnosti obdelave osebnih podatkov? Če da, kako pogosto jo posodabljate?

Ne, ne vodimo.

C3 in C4 Kako določate in nadzorujete roke hrambe dokumentacije z osebnimi podatki?

Mi rokov nimamo določenih v nekem internem pravilniku. Vendar dosledno vračamo dokumentacijo najkasneje vsake 2 leti po zaključku letnih poročil. Nekaterim vračamo tudi

vsako leto, če imajo dokumentacije več. Kar je pa v računalnikih pa imamo shranjeno za daljše obdobje, načeloma bolj ali manj trajno.

D1 Katere ukrepe ste uvedli za zagotovitev varnega prenosa, hrambe in dostopa do osebnih podatkov?

Imamo gesla na računalnikih in za v programe, vsaka stranka ima svoje geslo, gesla se razlikujejo tudi po modulih. Poslovne prostore zaklepamo in ključa ne dam zaposlenim dokler nisem res prepričana v njihovo delo in da jim lahko zaupam.

D2 Kako v vašem servisu zagotavljate, da do osebnih podatkov dostopajo le pooblaščene osebe?

Tako, da novih zaposlenih ne puščam samih v pisarni, tudi ključa nimajo svojega, vsi računalniki in papirji so vedno lahko rečemo »pod nadzorom«. Gesla za dostope dobivajo postopoma, ko se veča zaupanje. Do plač recimo, kjer je največ osebnih podatkov, dobijo dostop nazadnje.

D3 in D4 Katere IT–varnostne prakse uporabljate v svojem servisu? Na primer: ali imate vzpostavljeno dvofaktorsko prijavo, šifriranje pri pošiljanju dokumentov po e–pošti, redno varnostno kopiranje podatkov? Kje se ti podatki hranijo in kdo ima dostop do njih?

Dvofaktorske prijave za osebne podatke mislim, da nimamo nikjer, pošiljamo pa šifrirane dokumente po e pošti in delamo redne varnostne kopije podatkov, ampak na splošno vseh, ne ravno samo osebnih.

Kje se ti podatki hranijo in kdo ima dostop do njih?

Do podatkov ima dostop naš informatik in v teoriji tudi jaz, čeprav nikoli ne dostopam do njih. Shranjeni pa so v pisarni.

E1 Kako ocenjujete, da ste kot računovodski servis skladni z zakonodajo o varstvu osebnih podatkov – kateri vidiki so najbolj urejeni, kateri manj?

Nekje povprečno, zagotovo bi lahko bili bolj, lahko pa bi bili tudi še manj. Mislim, da z osebnimi podatki ravnamo skrbno, res redko pride do kakšnega neželenega dogodka, tako redko, da se ga zdaj iz glave niti ne spomnim nobenega. Bi pa zagotovo lahko na tem področju naredili še ogromno. Če ne drugega bi uredili vso potrebno dokumentacijo, določili roke hranjenja, pripravili pogodbe s poslovnimi partnerji in podobno.

E2 Ali ste že kdaj imeli notranjo ali zunanjo revizijo oz. nadzor s področja varstva osebnih podatkov? Kakšni so bili izsledki?

Ne še.

E3 in E4 Kako obravnavate zahteve posameznikov glede njihovih pravic? (dostop, popravek, izbris itd.)? Oz. kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

A prav posameznik, ki mu osebni podatki pripadajo?

Ja.

Izogibamo se komunikaciji s posamezniki. Raje vidimo, če gre za neko pooblaščeno osebno s strani poslovnega partnerja. Ampak seveda osebne podatke razkrijemo oz. popravimo.

E4 Kako bi ravnali v vašem računovodskem servisu, če bi posameznik pri vas želel uveljavljati svojo pravico do dostopa, popravka ali izbrisa osebnih podatkov?

Kot sem rekla se poskusimo temu izogniti. Raje vidimo če komunikacija poteka z našim poslovnim partnerjem in da potem oni posredujejo željene informacije naprej posameznikom.

E5 Ali imate kakšne postopke določene za primer, da posameznik neposredno naslovi zahtevo na vas, čeprav v praksi običajno nimate stika z njimi?

Samo ustno dogovorjene v podjetju. Na enak princip kot sem omenila. Poskusimo se izogniti komunikaciji s posamezniki. Če pa sodelavke kdaj glede česa niso prepričane pa potem vprašajo mene.

F1 Kaj so po vašem mnenju največji izzivi pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov v računovodskih servisih?

Težko rečem, ker o tem nisem še sploh razmišljala. Morda bi rekla da je na sploh izziv ostajati na tekočem z vsemi predpisi, ki jih moraš upoštevati kot podjetje in potem še posebej kot računovodstvo. Konkretno za varstvo osebnih podatkov pa ne vem, ker specifično za varstvo osebnih podatkov ne delamo nič drugače. Morda bomo do kakšnega izziva prišli enkrat kasneje, ko se bomo bolj sistematično lotili urejanja tega področja.

F2 Se vam zdi, da imate ustrezno dokumentacijo o obdelavi osebnih podatkov? Če ne, česa nimate?

Ne, nimamo ustrezne dokumentacije oz. je sploh nimamo.

F3 Ali imate morda narejeno oceno učinkov tveganja za zlorabo osebnih podatkov?

Ne.

F4 Če bi naredili oceno tveganja za zlorabo osebnih podatkov, kako bi ocenili, kje pri vas obstajajo največja tveganja in s kakšnimi vrstami tveganj se sploh soočate?

Ne bi rekla da so neka izrazita tveganja. Še najprej bi rekla, da se lahko zgodi, da pride do nekega neželenega razkritja napačni osebi. Pomotoma seveda.

G1 Kako je zakonodaja vplivala na vaše delovne procese in organizacijo dela?

Menim, da ni bistveno.

G2 Ste zaradi skladnosti z GDPR/ZVOP–2 uvedli kakšne nove storitve, postopke ali tehnologije?

Ne, nismo.