VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

ZASEBNO VAROVANJE IN GDPR: IZZIVI PRI OBDELAVI IN VAROVANJU OSEBNIH PODATKOV

Kandidat: Danjel Čebron

Vrsta študija: študent izrednega študija

Študijski program: Varovanje

Mentor predavatelj: Jakob Demšar, univ. dipl. prav.

Mentor v podjetju: Branko Debeljak

Lektorica: Maja Horvat, univ. dipl. slov.

Maribor, 2025

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Danjel Čebron sem avtor diplomskega dela z naslovom »Zasebno varovanje in GDPR: Izzivi pri obdelavi in varovanju osebnih podatkov«, ki sem ga napisal pod mentorstvom Jakoba Demšarja, univ. dipl. prav.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo - predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 - uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 - ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor: september 2025 Podpis študenta:

ZAHVALA

Iskrena hvala Višji strokovni šoli Academia Maribor ter vsem predavateljem za strokovno znanje, predanost in podporo, ki so pomembno prispevali k moji osebni in strokovni rasti.

Posebej se zahvaljujem mentorju na šoli, g. Jakobu Demšarju, univ. dipl. prav., za potrpežljivost, dragocene usmeritve in podporo ter mentorju podjetju, g. Branku Debeljaku, za praktične nasvete in pomoč pri povezovanju teorije s prakso.

Najgloblja hvala pa gre moji družini za razumevanje, spodbudo in neomajno podporo v celotnem obdobju študija.

POVZETEK

Diplomsko delo obravnava skladnost zasebno-varnostne dejavnosti z zahtevami varstva osebnih podatkov. Namen raziskave je bil ugotoviti, kako podjetje Hit d. d. Nova Gorica uresničuje določbe Splošne uredbe o varstvu podatkov (GDPR) in Zakona o varstvu osebnih podatkov (ZVOP-2) ter kateri so glavni izzivi v praksi.

Zasebno-varnostna podjetja dnevno obdelujejo identifikacijske podatke, evidence dostopa in videoposnetke, zato je skladnost z zakonodajo ključna za preprečevanje kršitev zasebnosti in pravnih posledic. Raziskava je temeljila na deskriptivni in analitični metodi, pregledu zakonodaje in internih postopkov podjetja ter kvalitativni presoji izkušenj iz prakse. Posebna pozornost je bila namenjena videonadzoru, pristopni kontroli, nadzoru zaposlenih in usposobljenosti osebja.

Analiza je pokazala, da ima podjetje večino ključnih postopkov urejenih na visoki ravni. Organizacijski in tehnični ukrepi, kot so nadzor dostopa do evidenc, varna hramba arhivov ter notranje revizije, so jasno opredeljeni in učinkovito izvajani, revizije pa so prispevale k izboljšavam evidentiranja in nadzora. Kljub pozitivnim rezultatom so bile zaznane pomanjkljivosti, predvsem pomanjkanje formalnih usposabljanj zaposlenih o GDPR.

Hipoteze so bile večinoma potrjene. GDPR je pomembno vplival na poslovanje varnostnih podjetij, zlasti pri videonadzoru, kjer se pojavljajo dileme glede zakonitosti in sorazmernosti obdelave podatkov. Medtem ko imajo nekateri izvajalci zasebnega varovanja še težave s celovitim pristopom k varstvu osebnih podatkov, podjetje Hit d. d. Nova Gorica izstopa po urejenosti postopkov in odgovornem ravnanju. Rezultati potrjujejo, da podjetja, ki vlagajo v nadzorne mehanizme in razvijajo kulturo varstva podatkov, dolgoročno dosegajo večjo uspešnost, konkurenčnost, ugled in zaupanje uporabnikov.

Delo prispeva k razumevanju razkoraka med zakonskimi zahtevami in prakso v varnostni dejavnosti ter nudi usmeritve za izboljšave. Poudarja tudi nujnost stalnega strokovnega razvoja varnostnega osebja, ki vsakodnevno ravna z občutljivimi podatki. Ugotovitve so lahko v pomoč tudi drugim izvajalcem zasebnega varovanja pri doseganju večje skladnosti in zmanjševanju tveganj pri obdelavi osebnih podatkov.

Ključne besede: *zasebno varovanje, varstvo osebnih podatkov, GDPR, ZVOP-2, videonadzor, skladnost s predpisi, Hit d. d. Nova Gorica*

ABSTRACT

“Private security and gdpr: challenges in processing and protecting personal data”

The diploma thesis examines the compliance of private security activities with personal data protection requirements. The aim of the research was to determine how Hit d. d. Nova Gorica implements the provisions of the General Data Protection Regulation (GDPR) and the Personal Data Protection Act (ZVOP-2), and to identify the main challenges in practice.

Private security companies process identification data, access records and video footage on a daily basis, making compliance with legislation crucial to prevent privacy breaches and serious legal consequences. The research applied descriptive and analytical methods, a review of legislation and internal company procedures, as well as a qualitative assessment of practical experience. Particular attention was given to video surveillance, access control, employee monitoring and staff training.

The analysis showed that the company has most key procedures well established. Organisational and technical measures such as access control, secure storage of archives and internal audits are clearly defined and effectively implemented, while audits have contributed to further improvements in record-keeping and monitoring. Despite the positive findings, some shortcomings were identified, especially the lack of formal GDPR training for staff.

The hypotheses were mostly confirmed. GDPR has significantly influenced the operations of security companies, particularly in the field of video surveillance, where dilemmas regarding the legality and proportionality of data processing are most common. While some private security providers still face difficulties in adopting a comprehensive approach to data protection, Hit d. d. Nova Gorica stands out for its well-regulated procedures and responsible conduct. The results confirm that companies investing in control mechanisms and fostering a culture of data protection achieve greater long-term success, competitiveness, reputation, customer trust and service quality.

This thesis contributes to understanding the gap between legal requirements and practical implementation in the security sector. The findings may also assist other private security providers seeking to enhance compliance and reduce risks in personal data processing.

Keywords: *private security, personal data protection, GDPR, ZVOP-2, video surveillance, regulatory compliance, Hit d. d. Nova Gorica*

KAZALO VSEBINE

1 UVOD 9

1.1 Opredelitev teme 9
1.2 Namen in cilji diplomskega dela 9
1.3 Raziskovalna vprašanja in hipoteze 9
1.4 Metodologija dela 10
1.5 Struktura diplomskega dela 10

2 TEORETIČNI OKVIR: GDPR IN ZVOP-2 12

2.1 Uredba GDPR 12
2.1.1 Temeljna načela obdelave osebnih podatkov 12
2.1.2 Zakonite podlage za obdelavo 12
2.1.3 Pravice posameznikov 13
2.1.4 Teritorialna veljavnost in vpliv izven EU 13
2.1.5 Kazni in odgovornost 13
2.2 Zakon o varstvu osebnih podatkov (ZVOP-2) 14
2.2.1 Posebnosti ZVOP-2 glede na GDPR 14
2.2.2 Vzpostavitev DPO in evidence dejavnosti obdelave 15
2.2.3 Nadzor in sankcije 15
2.2.4 Vpliv ZVOP-2 na zasebno varovanje 16
2.3 Razlika med upravljavcem in obdelovalcem osebnih podatkov 16
2.3.1 Upravljavec osebnih podatkov 16
2.3.2 Obdelovalec osebnih podatkov 16
2.3.3 Medsebojno razmerje in pogodba o obdelavi 17
2.3.4 Pomembnost razlikovanja v praksi 17
2.4 Pravni položaj izvajalca zasebnega varovanja v skladu z zakonom 17
2.4.1 Zakonska ureditev dejavnosti zasebnega varovanja 18
2.4.2 Licenca in odgovornost 18
2.4.3 Vloga izvajalcev kot upravljavcev ali obdelovalcev 18
2.4.4 Posegi v zasebnost in sorazmernost 19
2.5 Vloga informacijskega pooblaščenca 19
2.5.1 Pristojnosti in naloge 19
2.5.2 Vloga pri zasebnem varovanju 20
2.5.3 Sodelovanje z upravljavci in obdelovalci 20
2.5.4 Vloga v prihodnosti 21

3 ZASEBNO VAROVANJE IN OBDELAVA OSEBNIH PODATKOV 22

3.1 Dovoljene dejavnosti zasebnega varovanja in pravni okvir 22
3.1.1 Zakonski okvir 22
3.1.2 Vrste dovoljenih varnostnih storitev 22
3.1.3 Omejitve in nadzor nad dejavnostjo 23
3.1.4 Povezava s pravico do zasebnosti 23
3.2 Vrste osebnih podatkov, ki se zbirajo v okviru zasebnega varovanja 23
3.2.1 Opredelitev osebnih podatkov 24
3.2.2 Najpogosteje zbirani osebni podatki 24
3.2.3 Zakonitost zbiranja podatkov 25
3.3 Najpogostejše evidence in postopki (npr.: evidence video nazora, evidence pritožb, evidence izdanih sezam kartic) 25
3.3.1 Evidence v okviru zasebnega varovanja 26
3.3.2 Zakonitost in skladnost vodenja evidenc 27
3.4 Uporaba video nadzora v zasebnem varovanju 28
3.4.1 Pravna podlaga za izvajanje videonadzora 28
3.4.2 Tehnični in organizacijski ukrepi 29
3.4.3 Najpogostejše napake in kršitve v praksi 29
3.4.4 Pomen zakonitega videonadzora v zasebnem varovanju 30
3.5 Posebnosti obdelave osebnih podatkov pri nadzoru zaposlenih in obiskovalcev 30
3.5.1 Nadzor zaposlenih 30
3.5.2 Nadzor obiskovalcev 31

4 EVIDENTIRANJE IN OBDELAVA OSEBNIH PODATKOV V PODJETJU HIT D. D. NOVA GORICA 33

4.1 Predstavitev podjetja Hit d. d. in njegove varnostne službe 33
4.1.1 Naloge varnostne službe v kontekstu obdelave osebnih podatkov 33
4.1.2 Tehnično in organizacijsko varovanje podatkov 34
4.1.3 Skladnost s pravnim okvirom 35
4.2 Evidentiranje in obdelava osebnih podatkov pri opravljanju varnostnih storitev 36
4.2.1 Vrste evidenc in njihova zakonitost 36
4.2.2 Varnostni ukrepi in dostop do evidenc 37
4.2.3 Operativni postopki in odgovornosti 38
4.2.4 Izzivi pri vsakodnevnem delu 38
4.3 Uporaba video nadzora v praksi (tehnični in organizacijski vidiki) 39
4.3.1 Namen in obseg videonadzora 40
4.3.2 Pravna podlaga in skladnost z zakonodajo 40
4.3.3 Tehnična zasnova sistema 40
4.4 Izkušnje zaposlenih glede spoštovanja GDPR pri vsakodnevnem delu 41
4.4.1 Raven ozaveščenosti zaposlenih 41

4.4.2 Pogoste dileme in težave v praksi *42*
4.4.3 Notranje usposabljanje in izboljšave *42*
4.4.4 Odnos zaposlenih do varstva podatkov *43*
5 PRAKTIČNI IZZIVI IN ANALIZE **44**
5.1 SKLADNOST OBDELAVE PODATKOV Z GDPR IN ZVOP-2 V PODJETJU HIT D. D. 44
5.2 UGOTOVLJENE POMANJKLJIVOSTI IN TVEGANJA 45
5.2.1 Neenotna praksa vodenja evidenc *45*
5.2.2 Dvomi pri obravnavi zahtev posameznikov *45*
5.2.3 Omejena tehnična zaščita pri nekaterih evidencah *45*
5.3 PRIMERJAVA S PRIPOROČILI INFORMACIJSKEGA POOBLAŠČENCA 45
6 PRIPOROČILA ZA IZBOLJŠAVO **47**
6.1 PREDLOGI ZA IZBOLJŠANJE SKLADNOSTI Z ZAKONODAJO 47
6.2 IZOBRAŽEVANJE ZAPOSLENIH IN OZAVEŠČANJE 47
6.3 TEHNIČNE REŠITVE ZA VEČJO VARNOST PODATKOV 48
7 SKLEP **49**
8 LITERATURA **51**

KAZALO SLIK

SLIKA 1: OBVESTILO O IZVAJANJU VIDEO NADZORA V PODJETJU HIT D. D. 44

KAZALO TABEL

TABELA 1: PRIMERJAVA ZVOP-2 IN GDPR 15

1 UVOD

1.1 Opredelitev teme

V sodobni družbi, kjer se tehnologija in nadzor vse bolj prepletata z vsakdanjim življenjem, postaja vprašanje varovanja osebnih podatkov eno pomembnejših področij tudi v dejavnosti zasebnega varovanja. Varnostna podjetja vsakodnevno obdelujejo osebne podatke obiskovalcev, zaposlenih in drugih oseb, pri čemer morajo ravnati v skladu z zakonodajnimi predpisi, predvsem s Splošno uredbo o varstvu podatkov (GDPR, 2016) in Zakonom o varstvu osebnih podatkov (ZVOP-2, 2022).

Diplomsko delo obravnava praktične izzive pri obdelavi osebnih podatkov v okviru dejavnosti zasebnega varovanja s posebnim poudarkom na praksi v podjetju Hit d. d. Nova Gorica, kjer sem zaposlen kot skupinovodja varnostnikov. Namen dela je povezati pravni okvir z izvajanjem varstva osebnih podatkov na terenu ter podati pregled, kako zasebno-varnostna podjetja zagotavljajo skladnost z zahtevami GDPR.

1.2 Namen in cilji diplomskega dela

Namen diplomskega dela je proučiti zakonodajo, ki ureja obdelavo osebnih podatkov v dejavnosti zasebnega varovanja, ter analizirati, kako se ta pravila uporabljajo v praksi. Glavni cilji dela so:

- analizirati določbe GDPR in ZVOP-2, ki se nanašajo na varnostno dejavnost (ZVOP-2);
- proučiti, katere osebne podatke obdelujejo izvajalci zasebnega varovanja in zakaj;
- prikazati, kako je varstvo osebnih podatkov urejeno v podjetju Hit d. d.;
- izpostaviti izzive in predlagati možne izboljšave;
- preveriti hipoteze o stanju skladnosti v panogi zasebnega varovanja.

1.3 Raziskovalna vprašanja in hipoteze

Diplomsko delo temelji na naslednjih raziskovalnih vprašanjih:

- Kako se uredba GDPR uporablja v dejavnosti zasebnega varovanja?
- Katere osebne podatke obdelujejo izvajalci zasebnega varovanja in kako jih zavarujejo?

- S kakšnimi izzivi se srečujejo zasebno-varnostna podjetja pri zagotavljanju skladnosti z GDPR?

Na tej osnovi postavljam naslednje hipoteze:

H1: Večina podjetij za zasebno varovanje nima vzpostavljenega celovitega sistema varovanja osebnih podatkov.

H2: Uredba GDPR je bistveno vplivala na postopke zbiranja in hrambe podatkov v zasebnem varovanju.

H3: Varnostna podjetja, vključno s Hit d. d., se srečujejo z izzivi predvsem pri uporabi videonadzora v skladu z GDPR.

1.4 Metodologija dela

Raziskava temelji na kvalitativnem pristopu, saj je cilj razumeti zakonodajni okvir ter primerjati pravne zahteve z dejanskim stanjem v podjetju Hit d. d. Uporabljene bodo naslednje metode:

- deskriptivna metoda za opis pravnih virov (GDPR, 2016; ZVOP-2, 2022; ZZasV-1, 2011);
- analitična metoda za primerjavo zakonskih določil s prakso;
- študija primera podjetja Hit d. d.;
- notranja analiza dokumentacije (politike, evidence, navodila);
- intervjuji oziroma neformalni pogovori z zaposlenimi, kjer je to mogoče.

Uporaba podatkov bo skladna z etičnimi načeli, vsi osebni podatki bodo varovani, soglasja pa pridobljena v skladu z zahtevami GDPR.

1.5 Struktura diplomskega dela

Diplomsko delo je razdeljeno na osem poglavij. Po uvodnem delu sledi teoretični okvir, ki vključuje pregled GDPR, ZVOP-2, razliko med upravljavcem in obdelovalcem, pravni položaj varnostnih izvajalcev ter vlogo informacijskega pooblaščenca (GDPR, 2016; ZVOP-2, 2022).

V osrednjem delu sledi analiza dovoljenih dejavnosti zasebnega varovanja, vrst osebnih podatkov, ki se obdelujejo, in postopkov, kot so videonadzor, vodenje evidenc in nadzor nad zaposlenimi. Poseben poudarek je namenjen primeru podjetja Hit d. d., kjer so predstavljeni organizacijski in tehnični vidiki obdelave podatkov.

Zaključna poglavja vključujejo analizo praktičnih izzivov, priporočila za izboljšave, zaključek s potrditvijo hipotez, osebni prispevek ter predlog za nadaljnje raziskave. Delo se zaključi z navedbo literature po standardu APA.

2 TEORETIČNI OKVIR: GDPR IN ZVOP-2

2.1 Uredba GDPR

Varstvo osebnih podatkov je v sodobni digitalni dobi postalo eno pomembnejših področij pravnega urejanja, zlasti v luči naraščajočega obsega in kompleksnosti obdelave osebnih podatkov. Splošna uredba o varstvu podatkov (angl. General Data Protection Regulation, v nadaljevanju: GDPR) je temeljni pravni akt Evropske unije na področju varstva osebnih podatkov, ki se uporablja od 25. maja 2018.

GDPR ima neposreden učinek v vseh državah članicah EU, kar pomeni, da se uporablja brez prenosa v nacionalno zakonodajo. Namen uredbe je zagotoviti visoko in enotno raven varstva osebnih podatkov ter okrepiti pravice posameznikov glede njihove informacijske zasebnosti. Poleg tega uredba določa strožje obveznosti za organizacije, ki obdelujejo osebne podatke, ter bistveno povečuje odgovornost za kršitve varstva podatkov.

2.1.1 Temeljna načela obdelave osebnih podatkov

Člen 5 GDPR določa ključna načela, ki jih morajo upravljavci in obdelovalci osebnih podatkov upoštevati pri vsakršni obdelavi. Ta načela vključujejo:

- zakonitost, poštenost in preglednost,
- omejitev namena,
- minimizacijo podatkov,
- točnost,
- omejitev shranjevanja,
- celovitost in zaupnost,
- odgovornost.

Spoštovanje teh načel je osnova za zagotovitev skladnosti z GDPR in preprečevanje neupravičene ali čezmerne obdelave podatkov (GDPR, 2016).

2.1.2 Zakonite podlage za obdelavo

Obdelava osebnih podatkov je dopustna le, če je izpolnjena ena izmed zakonsko določenih pravnih podlag, opredeljenih v 6. členu GDPR. Te vključujejo:

- privolitev posameznika,

- izvajanje pogodbe,
- zakonska obveznost,
- zaščita življenjskih interesov,
- izvajanje nalog v javnem interesu ali pri izvajanju javne oblasti,
- zakoniti interesi upravljavca ali tretje osebe.

Organizacije, ki obdelujejo osebne podatke, morajo natančno določiti in dokumentirati, na kateri pravni podlagi temelji njihova obdelava (GDPR, 2016).

2.1.3 Pravice posameznikov

GDPR bistveno krepi pravice posameznikov glede lastnih osebnih podatkov. Med ključne pravice sodijo:

- pravica do dostopa do podatkov,
- pravica do popravka,
- pravica do izbrisa (pravica do pozabe),
- pravica do omejitve obdelave,
- pravica do prenosljivosti podatkov,
- pravica do ugovora obdelavi,
- pravica, da posameznika ne zadeva odločitev, ki temelji izključno na avtomatizirani obdelavi, vključno z oblikovanjem profilov.

Organizacije morajo te pravice posameznikom jasno predstaviti, omogočiti njihovo uresničevanje in se na zahteve pravočasno odzvati (GDPR, 2016).

2.1.4 Teritorialna veljavnost in vpliv izven EU

GDPR se ne uporablja le za organizacije s sedežem v EU, temveč tudi za tiste izven EU, če obdelujejo osebne podatke posameznikov v EU v okviru ponujanja blaga ali storitev ali spremljanja njihovega vedenja (GDPR, 2016, 3. člen). To pomeni, da ima uredba pomemben eksteritorialni učinek in vpliva na globalne prakse obdelave podatkov (GDPR, 2016).

2.1.5 Kazni in odgovornost

V primeru neskladnosti z določbami GDPR so predvidene visoke upravne globe, in sicer do 20 milijonov evrov ali 4 % celotnega svetovnega letnega prometa podjetja – kar je višje (GDPR, 2016, 83. člen). To poudarja pomen odgovornosti upravljavcev in obdelovalcev osebnih

podatkov ter nujnost vzpostavitve ustreznih varnostnih ukrepov, internih politik in dokumentacije (GDPR, 2016).

2.2 Zakon o varstvu osebnih podatkov (ZVOP-2)

Zakon o varstvu osebnih podatkov (ZVOP-2) predstavlja nacionalni pravni akt, ki v Republiki Sloveniji podrobneje ureja področja varstva osebnih podatkov, ki jih Splošna uredba o varstvu podatkov (GDPR) bodisi izrecno prepušča državam članicam bodisi jih ne ureja v celoti. ZVOP-2 je bil sprejet decembra 2022 in je začel veljati 26. januarja 2023, s čimer je nadomestil dotlej veljavni ZVOP-1 iz leta 2004 (GDPR, 2016; ZVOP-2, 2022; ZVOP-1, 2007).

Temeljni cilj zakona je zagotoviti učinkovito izvajanje in dopolnitev določb uredbe GDPR v slovenskem pravnem prostoru, hkrati pa urediti tudi tista področja, ki jih evropska uredba ne obravnava celovito, kot so videonadzor, biometrija, obdelava podatkov v delovnem razmerju, obdelava za namene znanstvenoraziskovalnega dela, novinarstva in drugo.

2.2.1 Posebnosti ZVOP-2 glede na GDPR

ZVOP-2 vpeljuje vrsto posebnih pravil, ki so pomembna predvsem za zasebne in javne subjekte pri vsakodnevni obdelavi osebnih podatkov (ZVOP-2, 2022):

Videonadzor: zakon podrobno ureja pogoje za zakonito izvajanje videonadzora tako v delovnih prostorih kot v javnem prostoru. Posebej sta poudarjeni prepoved prikritega videonadzora, razen v izjemnih primerih (npr. kazniva dejanja), ter obveznost označevanja nadzorovanega območja (ZVOP-2, 2022, 76.–80. člen).

Biometrija: biometrične ukrepe (npr. prepoznavo obraza, prstne odtise) je dopustno izvajati le pod zelo omejenimi pogoji in ob sorazmernosti glede na namen obdelave.

Obdelava v delovnih razmerjih: zakon določa, da mora biti obdelava osebnih podatkov zaposlenih nujna in sorazmerna ter ne sme posegati v njihovo zasebnost bolj, kot je to nujno za dosego zakonitega cilja (ZVOP-2, 2022, 89. člen).

Posebni režimi za javni sektor: ZVOP-2 določa tudi posebna pravila za državne organe, občine, javne zavode in druga telesa javnega sektorja, ki so podvrženi strožjim omejitvam pri obdelavi osebnih podatkov (ZVOP-2, 2022).

Tabela 1: Primerjava ZVOP-2 in GDPR

Področje	GDPR	ZVOP-2
Nadzorni organ	Nacionalni nadzorni organi vsake države članice (v Sloveniji IP RS)	Informacijski pooblaščenec RS
Uveljavitev	25. maj 2018	26. januar 2023
Veljavnost	Neposredno zavezujoča v vseh članicah EU	Nacionalni zakon, ki dopolnjuje GDPR
Ocena učinka (DPIA)	Obvezna za nekatere vrste obdelave (člen 35)	Dopolnjuje in natančneje določa obveznosti glede DPIA
Videonadzor	Splošna pravila o zakonitosti in sorazmernosti	Podrobna določila v členih 76–80
Kazen za kršitve	Do 20 mio EUR ali 4 % letnega prometa	Enake kazni kot GDPR, ker je dopolnitev GDPR

Vir: (ZVOP-2, 2022)

2.2.2 Vzpostavitev DPO in evidence dejavnosti obdelave

Zakon skladno z GDPR določa obveznost določitve pooblaščene osebe za varstvo podatkov (Data Protection Officer – DPO) za določene organizacije, zlasti v javnem sektorju in pri obsežni obdelavi posebnih vrst podatkov. Poleg tega zakon predpisuje vodenje evidence dejavnosti obdelave kot temeljnega dokumenta, ki omogoča sledljivost in preglednost obdelave (GDPR, 2016).

2.2.3 Nadzor in sankcije

Za nadzor nad izvajanjem ZVOP-2 in GDPR je pristojen Informacijski pooblaščenec RS kot samostojen in neodvisen nadzorni organ. Pooblaščenec lahko izvaja nadzore, izdaja zavezujoče odločbe, opozorila in tudi upravne globe (GDPR, 2016; ZVOP-2, 2022).

Globe so v ZVOP-2 usklajene z določbami GDPR – v primeru hudih kršitev lahko znašajo do 20 milijonov evrov ali 4 % letnega prometa pravne osebe, odvisno od narave kršitve (GDPR, 2016, 83. člen; ZVOP-2, 2022).

2.2.4 Vpliv ZVOP-2 na zasebno varovanje

Za področje zasebnega varovanja je ZVOP-2 posebej pomemben pri obravnavi videonadzora, obdelavi podatkov obiskovalcev in zaposlenih ter vodenju posebnih evidenc (npr. evidenc dostopov, pritožb, ukrepov varnostnika). V praksi mora izvajalec zasebnega varovanja ravnati v skladu z določili zakona, kar pomeni zagotavljanje minimalnega obsega podatkov, jasno informiranje posameznikov ter izvajanje tehničnih in organizacijskih ukrepov za zaščito informacij (ZVOP-2, 2022).

2.3 Razlika med upravljavcem in obdelovalcem osebnih podatkov

Jasna razmejitev med upravljavcem in obdelovalcem osebnih podatkov je eden izmed temeljnih konceptov, ki jih uvaja Splošna uredba o varstvu podatkov (GDPR). Razlikovanje med obema vlogama ima pomembne pravne posledice, saj GDPR določa različne obveznosti in stopnje odgovornosti za vsako vlogo posebej (GDPR, 2016, člen 4).

2.3.1 Upravljavec osebnih podatkov

Upravljavec (angl. controller) je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki samostojno ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov (GDPR, 2016, člen 4(7)). To pomeni, da ima upravljavec odločilno vlogo pri tem, zakaj in kako se bodo osebni podatki obdelovali (GDPR, 2016).

V praksi so upravljavci pogosto podjetja, državne institucije ali druge organizacije, ki zbirajo osebne podatke zaradi izpolnjevanja svojih nalog ali storitev – na primer delodajalec, ki vodi evidenco o zaposlenih, ali zdravstvena ustanova, ki vodi kartoteko pacientov.

Upravljavci so v skladu z GDPR primarno odgovorni za skladnost z zakonodajo. To vključuje izvajanje načel varstva podatkov, zagotavljanje pravic posameznikov, vodenje evidenc dejavnosti obdelave, imenovanje pooblaščene osebe (DPO), izvajanje ocen učinkov na varstvo podatkov (DPIA) in sodelovanje z nadzornim organom.

2.3.2 Obdelovalec osebnih podatkov

Obdelovalec je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca (GDPR, 2016, člen 4(8)). Obdelovalec sam ne določa namenov ali sredstev obdelave, temveč izvaja dejanja obdelave zgolj na osnovi pogodbe ali drugega pravnega akta, ki ga sklene z upravljavcem (GDPR, 2016).

Primer obdelovalca je podjetje, ki upravlja informacijski sistem za naročnika (upravljavca), ali izvajalec zasebnega varovanja, ki vodi evidenco obiskovalcev v imenu naročnika storitve.

Obdelovalec je dolžan upoštevati navodila upravljavca, hkrati pa mora sam poskrbeti za ustrezne tehnične in organizacijske ukrepe, ki zagotavljajo varnost osebnih podatkov, ki jih obdeluje.

2.3.3 Medsebojno razmerje in pogodba o obdelavi

Med upravljavcem in obdelovalcem mora biti sklenjena pogodba o obdelavi osebnih podatkov, ki natančno določa predmet, trajanje, naravo in namen obdelave, vrste osebnih podatkov, kategorije posameznikov ter pravice in obveznosti obeh strank (GDPR, 2016, člen 28).

Pogodba mora vsebovati tudi določila o zaupnosti, varnosti, morebitni vključitvi podobdelovalcev ter obveznosti vračila ali uničenja podatkov po koncu sodelovanja.

2.3.4 Pomembnost razlikovanja v praksi

V praksi je pravilna identifikacija upravljavca in obdelovalca zelo pomembna, saj vpliva na:

- odgovornost v primeru kršitev,
- porazdelitev obveznosti glede varovanja pravic posameznikov,
- vodenje evidenc dejavnosti obdelave,
- določitev, kdo je dolžan izvesti oceno učinka na varstvo podatkov (DPIA).

V kontekstu zasebnega varovanja se podjetje, ki najame zunanjo varnostno službo, praviloma šteje za upravljavca, medtem ko je varnostna služba obdelovalec, razen če sama določa namen in sredstva obdelave – v tem primeru lahko nastopa kot samostojen upravljavec.

2.4 Pravni položaj izvajalca zasebnega varovanja v skladu z zakonom

Izvajalci zasebnega varovanja so pravne ali fizične osebe, ki opravljajo naloge varovanja oseb in premoženja za naročnike v skladu z določbami Zakona o zasebnem varovanju (ZZasV-1, 2011). Gre za specifično gospodarsko dejavnost, ki je podvržena strogi zakonski regulaciji, saj neposredno posega v pravice posameznikov, vključno z varstvom osebnih podatkov, zasebnostjo in svobodo gibanja (ZZas-1, 2011).

2.4.1 Zakonska ureditev dejavnosti zasebnega varovanja

Zakon o zasebnem varovanju (ZZasV-1, 2011) opredeljuje vrste varnostnih storitev (varovanje ljudi in premoženja, varovanje oseb, prevoz in varovanje gotovine ter drugih vrednostnih pošiljk, varovanje javnih zbiranj, varovanje prireditev v gostinskih lokalih, upravljanje z varnostno-nadzornim centrom – VNC, načrtovanje sistemov tehničnega varovanja, izvajanje sistemov tehničnega varovanja), pogoje za opravljanje dejavnosti, izdajo licenc, nadzor nad delovanjem izvajalcev ter dolžnosti varnostnega osebja (ZZasV-1, 2011).

Z vidika varstva osebnih podatkov so pomembne predvsem naslednje določbe:

- izvajanje videonadzora v varovanih prostorih,
- vodenje evidenc obiskovalcev in dostopov, preverjanje identitete oseb (z dokumenti),
- poročanje o incidentih in varnostnih dogodkih.

V vseh teh postopkih prihaja do sistematične obdelave osebnih podatkov, zato mora izvajalec varovanja delovati v skladu z določili GDPR in ZVOP-2 (GDPR, 2016; ZVOP-2, 2022).

2.4.2 Licenca in odgovornost

Vsak izvajalec zasebnega varovanja mora pridobiti licenco, ki jo izda Ministrstvo za notranje zadeve, ter voditi evidenco zaposlenih, preverjati nekaznovanost in ustrezno usposobljenost varnostnega osebja. Poleg tega mora izvajati nadzor nad varnostniki ter zagotavljati ustrezno dokumentacijo in tehnične pogoje za izvajanje storitev.

Izvajalci so dolžni:

- uporabljati osebne podatke le v obsegu in za namen, ki je nujen za izvajanje storitev,
- zagotoviti informiranje posameznikov o obdelavi njihovih podatkov (npr. z obvestili o videonadzoru ali informacijskimi tablami),
- sprejeti ustrezne tehnične in organizacijske ukrepe za varnost podatkov (šifriranje, dostopna pooblastila, varnostni protokoli),
- voditi evidence obdelave skladno s 30. členom GDPR.

2.4.3 Vloga izvajalcev kot upravljavcev ali obdelovalcev

Položaj izvajalca zasebnega varovanja kot upravljavca ali obdelovalca osebnih podatkov je odvisen od konkretnega pogodbenega razmerja z naročnikom:

- Če izvajalec samostojno določa namen in sredstva obdelave (npr. lastni sistem videonadzora v svojih poslovnih prostorih), nastopa kot upravljavec;

- Če pa varnostno podjetje deluje v imenu naročnika in v skladu z njegovimi navodili (npr. izvaja videonadzor za naročnika), je obdelovalec;
- V primeru podjetja Hit d. d., ki ima lastno interno varnostno službo, podjetje kot celota nastopa kot upravljavec osebnih podatkov. Interna varnostna služba v tem primeru ne deluje kot samostojen upravljavec ali pogodbeni obdelovalec, temveč kot notranja organizacijska enota, ki izvaja obdelavo v imenu upravljavca, torej podjetja Hit d. d.

V vsakem primeru pa ima izvajalec zakonsko odgovornost za zakonitost obdelave, spoštovanje pravic posameznikov in zaščito zbranih osebnih podatkov.

2.4.4 Posegi v zasebnost in sorazmernost

Izvajalci morajo pri svojem delu spoštovati načelo sorazmernosti, kar pomeni, da smejo poseči v pravice posameznikov (npr. zbiranje osebnih podatkov, preverjanje identitete, nadzor s kamerami) le v obsegu, ki je nujno potreben za zagotovitev varnosti. Neupravičeno zbiranje podatkov, predolgo shranjevanje ali prikriti nadzor lahko predstavljajo kršitev GDPR in ZVOP-2 (GDPR, 2016; ZVOP-2, 2022).

V praksi je pomembno tudi, da se izvaja notranji nadzor nad ravnanjem z osebnimi podatki in da se varnostno osebje ustrezno izobražuje o zakonodaji ter etičnih vidikih dela z informacijami.

2.5 Vloga informacijskega pooblaščenca

Informacijski pooblaščenec Republike Slovenije (IP) je neodvisen državni organ, pristojen za nadzor nad izvajanjem zakonodaje na področju varstva osebnih podatkov. Delovanje IP temelji na določbah GDPR (členi 51 in naslednji), ZVOP-2 ter Zakona o dostopu do informacij javnega značaja (ZDIJZ), saj IP opravlja tudi funkcijo nadzora nad transparentnostjo javnega sektorja (GDPR, 2016; ZVOP-2, 2022).

2.5.1 Pristojnosti in naloge

Informacijski pooblaščenec ima v skladu z zakonodajo naslednje ključne pristojnosti (ZVOP-2, 2022; GDPR, 2016, člen 57):

- nadzor nad zakonitostjo obdelave osebnih podatkov v javnem in zasebnem sektorju,
- vodenje inšpekcijskih postopkov ter izrekanje ukrepov in upravnih glob,
- obravnavanje pritožb posameznikov glede kršitev njihovih pravic,
- izdaja smernic, mnenj in priporočil glede zakonite obdelave podatkov,

- ozaveščanje in izobraževanje javnosti, zlasti upravljavcev, obdelovalcev in posameznikov,
- sodelovanje z drugimi nadzornimi organi v EU v okviru Evropskega odbora za varstvo podatkov (EDPB).

Pooblaščenec lahko izreče več vrst ukrepov – od opozoril in odredb do denarnih kazni, ki so lahko skladno z GDPR zelo visoke (do 20 milijonov evrov oziroma 4 % letnega prometa podjetja) (GDPR, 2016).

2.5.2 Vloga pri zasebnem varovanju

Na področju zasebnega varovanja ima IP pomembno svetovalno in nadzorstveno vlogo. V praksi obravnava številne primere, povezane z:

- nezakonitim ali nesorazmernim videonadzorom (npr. snemanje javnih površin, snemanje zaposlenih brez pravne podlage),
- neustrezno informiranostjo posameznikov glede obdelave njihovih podatkov,
- nevarnim ravnanjem z evidencami (npr. dostop do podatkov brez ustreznih pooblastil),
- kršitvami pravic posameznikov, kot je pravica do dostopa ali izbrisa podatkov.

IP redno objavlja smernice in stališča, ki so v pomoč izvajalcem zasebnega varovanja pri zakonitem izvajanju dejavnosti. Med te dokumente sodijo:

- smernice za izvajanje videonadzora,
- mnenja o zakoniti obdelavi podatkov zaposlenih,
- stališča o hrambi in vodenju evidenc,
- odločbe in inšpekcijska poročila.

2.5.3 Sodelovanje z upravljavci in obdelovalci

IP spodbuja preventivno delovanje organizacij, kar pomeni, da naj se podjetja in javni organi še pred uvedbo novih postopkov (npr. uvedbo novega videonadzornega sistema) obrnejo nanj za mnenje ali posvet. Prav tako se pričakuje, da bodo večji upravljavci izvajali ocene učinka na varstvo podatkov (DPIA) v sodelovanju s pooblaščencem.

Organizacije lahko IP zaprosijo tudi za uradno mnenje, ki jim pomaga pri vzpostavitvi skladnosti z zakonodajo, še posebej v primerih, ko gre za kompleksnejše obdelave, kot so biometrija, avtomatizirano odločanje ali stalni nadzor zaposlenih.

2.5.4 Vloga v prihodnosti

Glede na razvoj digitalnih tehnologij, umetne inteligence in avtomatizacije nadzora bo vloga informacijskega pooblaščenca v prihodnje še pomembnejša, zlasti na področjih, kjer prihaja do množične ali občutljive obdelave podatkov, kar zasebno varovanje pogosto je.

3 ZASEBNO VAROVANJE IN OBDELAVA OSEBNIH PODATKOV

3.1 Dovoljene dejavnosti zasebnega varovanja in pravni okvir

Zasebno varovanje je posebna gospodarska dejavnost, ki se izvaja z namenom varovanja ljudi in premoženja. Zaradi občutljive narave teh nalog je dejavnost zasebnega varovanja v Sloveniji natančno opredeljena in urejena z zakonom, saj lahko vključuje pomembne posege v človekove pravice, zlasti v pravico do zasebnosti in varstva osebnih podatkov.

3.1.1 Zakonski okvir

Temeljna pravna podlaga za izvajanje zasebnega varovanja v Republiki Sloveniji je Zakon o zasebnem varovanju (ZZasV-1), ki je začel veljati leta 2011 (ZZasV-1, 2011).

Zakon natančno določa (ZZasV-1, 2011).:

- vrste in obseg dovoljenih varnostnih storitev,
- pogoje za pridobitev licence,
- obveznosti varnostnega osebja,
- nadzor nad delovanjem varnostnih služb,
- sodelovanje z javnimi organi (npr. policijo).

Poleg ZZasV-1 morajo izvajalci zasebnega varovanja upoštevati tudi ZVOP-2 in GDPR, kadar pri svojem delu obdelujejo osebne podatke (npr. identifikacija obiskovalcev, videonadzor, vodenje evidenc) (GDPR, 2016; ZZasV-1, 2011; ZVOP-2, 2022).

3.1.2 Vrste dovoljenih varnostnih storitev

ZZasV-1 v 3. členu določa, da se dejavnost zasebnega varovanja lahko izvaja le v obliki naslednjih licenciranih varnostnih storitev (ZZasV-1, 2011):

1. varovanje ljudi in premoženja;
2. varovanje oseb;
3. prevoz in varovanje gotovine ter drugih vrednostnih pošiljk;
4. varovanje javnih zbiranj;
5. varovanje prireditev v gostinskih lokalih;
6. upravljanje z varnostno-nadzornim centrom (VNC);

7. načrtovanje sistemov tehničnega varovanja;
8. izvajanje sistemov tehničnega varovanja.

Za izvajanje navedenih dejavnosti mora imeti podjetje veljavno licenco, posamezni varnostniki pa morajo biti ustrezno usposobljeni in imeti pridobljeno poklicno kvalifikacijo.

3.1.3 Omejitve in nadzor nad dejavnostjo

Zasebno varovanje se ne sme izvajati samovoljno ali zunaj zakonskih okvirov. Ključne omejitve vključujejo:

- prepoved prekoračitve pooblastil, kot so prisilna sredstva ali uporaba orožja brez zakonske podlage,
- prepoved prikritega delovanja,
- obveznost spoštovanja človekovih pravic, zlasti pravice do zasebnosti, dostojanstva in nedotakljivosti posameznika.

Za nadzor nad dejavnostjo je pristojno Ministrstvo za notranje zadeve, ki lahko izvede nadzore, začasno prepove izvajanje storitev ali odvzame licenco. Hkrati lahko Informacijski pooblaščenec nadzira zakonitost obdelave osebnih podatkov pri izvajanju varnostnih storitev.

3.1.4 Povezava s pravico do zasebnosti

Zasebno varovanje je dejavnost, ki se izvaja v »ravnotežju« med dvema pravicama: pravico do varnosti in pravico do zasebnosti. Pomembno načelo je, da morajo biti varnostni ukrepi sorazmerni, zakoniti in potrebni, da ne prihaja do neupravičenega poseganja v zasebno življenje posameznikov.

Zaradi tega morajo izvajalci dosledno spoštovati zakonodajo ter ravnati pregledno in odgovorno tako pri fizičnem varovanju kot pri uporabi tehnoloških sredstev (videonadzor, rentgen, kontrole pristopa ipd.).

3.2 Vrste osebnih podatkov, ki se zbirajo v okviru zasebnega varovanja

Izvajanje zasebnega varovanja neizogibno vključuje obdelavo različnih vrst osebnih podatkov, saj varnostno osebje pri opravljanju nalog pogosto beleži, obdeluje in hrani informacije o posameznikih – zaposlenih, obiskovalcih, strankah oziroma gostih ter tretjih osebah. Zato je poznavanje vrst podatkov, ki se pri tem zbirajo, pomembno za razumevanje obsega varstvenih obveznosti izvajalcev varovanja.

3.2.1 Opredelitev osebnih podatkov

V skladu z GDPR so osebni podatki vse informacije, ki se nanašajo na določeno ali določljivo fizično osebo. To vključuje tako neposredne identifikatorje (ime, priimek, naslov) kot tudi posredne (registrska številka, številka kartice, posnetek obraza) (GDPR, 2016).

V okviru zasebnega varovanja se najpogosteje zbirajo navadni osebni podatki, v določenih primerih pa tudi posebne vrste osebnih podatkov, za katere velja strožji režim obdelave (npr. biometrični podatki).

3.2.2 Najpogosteje zbirani osebni podatki

V zasebnem varovanju se obdelujejo naslednje skupine osebnih podatkov:

- Identifikacijski podatki posameznikov:
- ime in priimek,
- naslov stalnega ali začasnega prebivališča,
- številka osebnega dokumenta (v določenih primerih),
- registrska številka vozila (npr. na parkiriščih),
- podatki iz službene ali identifikacijske kartice.
- **Podatki o dostopih in gibanjih posameznikov:**
- datum, čas in kraj vstopa/izstopa,
- gibanje po objektu (npr. preko kartic ali kamer),
- spremljanje obiskov v varovanih prostorih,
- zgodovina dostopov.
- **Posnetki iz videonadzora:**
- vizualni posnetki posameznikov (npr. obrazi),
- vedenjski vzorci, gibanje po prostoru,
- v določenih primerih tudi zvok, če je to posebej dovoljeno (redko in pod strogimi pogoji).
- **Biometrični podatki (če se uporabljajo):**
- prstni odtisi,
- prepoznavanje obraza,
- mrežnica

  (ti podatki spadajo med posebne vrste osebnih podatkov in jih je dovoljeno obdelovati le pod posebnimi pogoji iz člena 9 GDPR in člena 83 ZVOP-2).

- **Podatki o dogodkih, incidentih in kršitvah:**
- osebni podatki v varnostnih poročilih, poškodbah, incidentih,
- podatki o posredovanju varnostnikov,
- izjave prič, časovni zapisi.
- **Podatki iz evidenc obiskovalcev/gostov in zaposlenih:**
- podatki iz vpisnih knjig (ime, priimek, čas obiska, podjetje),
- številka obiskovalčeve kartice,
- podpis za potrditev prisotnosti.
- **Ostali tehnični in spremljevalni podatki:**
- IP-naslovi uporabnikov v nadzornih sistemih,
- podatki iz alarmnih sistemov,
- lokacijski podatki (npr. GPS-nadzor nad službenimi vozili).

3.2.3 Zakonitost zbiranja podatkov

Zbiranje vseh zgoraj navedenih podatkov mora imeti jasno zakonsko podlago, kot določa 6. člen GDPR. V praksi to pomeni (GDPR, 2016):

- zakonita podlaga (npr. pogodba, zakon, zakoniti interes naročnika),
- spoštovanje načela sorazmernosti (zbirajo se samo nujno potrebni podatki),
- jasna informiranost posameznikov (npr. z obvestili, tabelami, obvestili o snemanjih),
- ustrezna hramba in zaščita teh podatkov.

V primeru obdelave posebnih vrst osebnih podatkov (npr. biometrija) mora obstajati ena od posebnih pravnih podlag iz 9. člena GDPR, kot so izrecna privolitev posameznika, nujnost za zaščito življenjskih interesov ali obdelava, ki je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca (GDPR, 2016).

3.3 Najpogostejše evidence in postopki (npr.: evidence video nazora, evidence pritožb, evidence izdanih sezam kartic)

Pri izvajanju dejavnosti zasebnega varovanja se ustvarjajo in vodijo različne evidence, namenjene zagotavljanju varnosti, preglednosti postopkov, odgovornosti ter skladnosti z zakonodajo. Ker te evidence pogosto vsebujejo osebne podatke posameznikov, morajo biti oblikovane in vodene v skladu z načeli GDPR in ZVOP-2, zlasti glede zakonitosti,

sorazmernosti, časovne omejitve hrambe ter pravice do dostopa in popravka (GDPR, 2016; ZVOP-2, 2022).

3.3.1 Evidence v okviru zasebnega varovanja

Najpogostejše evidence, ki jih vodi izvajalec zasebnega varovanja, so:

- **Evidence videonadzora:**

Videonadzor predstavlja enega najpogostejših ukrepov zasebnega varovanja, zato je z njim povezana tudi ustrezna evidenca obdelave, ki vključuje:

- lokacijo kamer,
- namen snemanja,
- območje snemanja,
- čas hrambe posnetkov,
- pooblaščene osebe.

GDPR zahteva, da je videonadzor sorazmeren in transparenten, kar vključuje obvezno obvestilo o nadzoru ter pravico posameznika do vpogleda v posnetke, če je na njih razpoznaven (GDPR, 2016, členi 12–15; Informacijski pooblaščenec RS, 2023a).

- **Evidence obiskovalcev:**

Zaradi varnosti prostorov se pogosto vodi evidenca vseh obiskovalcev, v kateri se beležijo:

- ime in priimek obiskovalca,
- čas prihoda in odhoda,
- podjetje ali razlog obiska,
- številka osebnega dokumenta (po potrebi).

Tovrstna evidenca mora biti ustrezno zavarovana, podatki pa se ne smejo hraniti dlje, kot je nujno za dosego namena (ZVOP-2, 2022, 43. člen; IP RS, 2023b). Priporočljivo je, da so obrazci elektronski ali zaklenjeni, da se prepreči neupravičeno razkritje podatkov naslednjim obiskovalcem (ZVOP-2, 2022).

- **Evidence izdanih identifikacijskih in sezam kartic:**

V številnih organizacijah izvajalci varovanja upravljajo z izdajo in vračanjem identifikacijskih ali dostopnih kartic (sezam kartic). Evidence običajno vključujejo:

- podatke o prejemniku kartice (ime, priimek, enota),

- datum izdaje in vračila,
- številko kartice,
- pooblastilo za dostop do določenih območij.

Z vidika varstva osebnih podatkov morajo imeti uporabniki jasno informacijo o namenih zbiranja teh podatkov in pravilih za njihovo uporabo (GDPR, 2016, člen 13; IP RS, 2023c; GDPR, 2016).

- **Evidence pritožb in ukrepov varnostnika:**

V primeru konfliktnih situacij, kršitev ali dogodkov, ki vključujejo posredovanje varnostnikov, se vodijo posebne evidence, ki lahko vsebujejo:

- osebne podatke vpletenih (ime, priimek, opis dogodka),
- čas in kraj dogodka,
- ukrepe, ki so bili izvedeni,
- izjave prič.

Takšni zapisi so posebej občutljivi in zahtevajo višjo stopnjo varovanja, saj pogosto vsebujejo tudi posebne vrste podatkov, kot so podatki o zdravstvenem stanju ali vedenjskih značilnostih posameznikov (ZVOP-2, 2022).

3.3.2 Zakonitost in skladnost vodenja evidenc

Vse evidence, ki vključujejo osebne podatke, morajo biti v skladu z načeli iz 5. člena GDPR (2016):

- obdelava mora biti zakonita, poštena in pregledna,
- podatki morajo biti zbrani za določen, izrecen in zakonit namen,
- hramba mora biti časovno omejena,
- zagotovljeni morajo biti ustrezni varnostni ukrepi.

Poleg tega mora organizacija voditi evidenco dejavnosti obdelave v skladu s 30. členom GDPR, kjer so navedeni vsi postopki in evidence, ki vključujejo obdelavo osebnih podatkov (GDPR, 2016).

3.4 Uporaba video nadzora v zasebnem varovanju

Videonadzor je ena najpogosteje uporabljenih metod zasebnega varovanja, saj omogoča spremljanje dogajanja v realnem času, dokumentiranje incidentov in povečevanje občutka varnosti. Hkrati pa gre za občutljivo obliko obdelave osebnih podatkov, saj lahko videoposnetki razkrijejo identiteto posameznika, njegovo gibanje, navade ali celo vedenje. Zaradi tega je videonadzor strogo urejen z GDPR in ZVOP-2, ki določata natančne pogoje in omejitve (GDPR, 2016; ZVOP-2, 2022).

3.4.1 Pravna podlaga za izvajanje videonadzora

- **Splošna uredba o varstvu podatkov (GDPR):**

GDPR v 4. členu videoposnetke, ki omogočajo prepoznavo posameznika, opredeljuje kot osebne podatke. Vsaka obdelava teh podatkov mora biti skladna z načeli iz 5. člena GDPR, med katerimi so:

- zakonitost, poštenost in preglednost,
- omejitev namena,
- minimizacija podatkov,
- omejena hramba,
- zaupnost in integriteta.

Najpogostejša pravna podlaga za izvajanje videonadzora v zasebnem varovanju je zakoniti interes upravljavca (GDPR, člen 6(1)(f)), kadar je snemanje nujno za zaščito ljudi ali premoženja (GDPR, 2016).

Upravljavec mora tudi:

- posameznikom zagotoviti informacijo o snemanju (člen 13),
- omogočiti vpogled v posnetke (člen 15),
- voditi evidenco dejavnosti obdelave (člen 30),
- izvesti oceno učinka na varstvo podatkov (DPIA), kadar gre za sistematični nadzor na javnih mestih (člen 35).

- **Zakon o varstvu osebnih podatkov (ZVOP-2):**

ZVOP-2 podrobneje ureja videonadzor v slovenskih pravnih okvirih in določa stroga pravila glede njegovega izvajanja (ZVOP-2, 2022):

- Videonadzor je dovoljen, če je nujno potreben za varnost ljudi, premoženja ali poslovnih skrivnosti (člen 76).
- Snemano območje mora biti vidno označeno z obvestilno tablo, ki vsebuje podatke o upravljavcu, kontakt za DPO (če obstaja), namen snemanja in druge zakonsko zahtevane podatke (člen 77).
- Najdaljše obdobje hrambe posnetkov je 30 dni, razen če je to potrebno za reševanje konkretnega incidenta (člen 76).
- Prikriti videonadzor (npr. brez obvestila) je prepovedan, razen v izjemnih primerih zaradi suma hudega kaznivega dejanja (člen 79).
- Na delovnem mestu je videonadzor dopusten le ob utemeljenem razlogu, kadar ni mogoče doseči varnostnega cilja z milejšimi sredstvi. Poleg tega ne sme biti usmerjen neposredno v delovna mesta zaposlenih (člen 78).

3.4.2 Tehnični in organizacijski ukrepi

Video nadzorni sistemi morajo biti upravljani na način, ki preprečuje nepooblaščen dostop, zlorabo ali razkritje posnetkov. Upravljavec mora zato vzpostaviti:

- fizično zaščito snemalnih naprav (zaklenjeni prostori, kontrola dostopa),
- dostop samo za pooblaščene osebe (knjiga o izvajanju z video nadzornim sistemom),
- šifriranje sledi, ki omogočajo revizijo dostopov,
- interni pravilnik o videonadzoru,
- pogodbo z obdelovalcem (če videonadzor izvaja zunanje podjetje – člen 28 GDPR; GDPR, 2016),
- ob tveganih obdelavah (npr. javne površine, delovna mesta) je obvezna tudi ocena učinkov na varstvo osebnih podatkov (DPIA) po 35. členu GDPR (2016).

3.4.3 Najpogostejše napake in kršitve v praksi

Informacijski pooblaščenec RS pogosto opozarja na tipične napake izvajalcev zasebnega varovanja, med katerimi so:

- neoznačenost nadzorovanih prostorov,
- predolgo hranjenje posnetkov brez utemeljitve,
- nedovoljen nadzor zaposlenih brez pravne podlage,
- nedosledno vodenje evidenc,
- neizpolnjevanje obveznosti informiranja posameznikov.

Takšne kršitve lahko vodijo do inšpekcijskega nadzora, odredb za izbris podatkov ali celo upravnih glob v skladu s členom 83 GDPR in 96. členom ZVOP-2 (GDPR, 2016; ZVOP-2, 2022).

3.4.4 Pomen zakonitega videonadzora v zasebnem varovanju

Videonadzor je učinkovit in legitimen varnostni ukrep, če je izveden skladno z zakonodajo. S tem se ne zaščitita le naročnik in njegovo premoženje, temveč tudi pravice posameznikov, zlasti pravica do zasebnosti in informacijske samoopredelitve.

Izvajalci zasebnega varovanja imajo zato dvojno odgovornost:

1. zagotavljati varnost oseb in objektov,
2. spoštovati temeljne pravice posameznikov, ki se znajdejo v nadzorovanem okolju.

3.5 Posebnosti obdelave osebnih podatkov pri nadzoru zaposlenih in obiskovalcev

Obdelava osebnih podatkov v okviru zasebnega varovanja pogosto vključuje tudi nadzor zaposlenih in spremljanje obiskovalcev, kar velja za posebej občutljivo področje z vidika varstva zasebnosti. Pri tem se upravljavci in izvajalci varovanja soočajo z vprašanji zakonitosti, sorazmernosti in nujnosti obdelave. Zaradi potencialnih posegov v temeljne pravice posameznikov zakonodaja določa strožje pogoje in varovalke.

3.5.1 Nadzor zaposlenih

- **Pravni okvir**

Videonadzor in druge oblike nadzora zaposlenih predstavljajo resen poseg v pravico do zasebnosti na delovnem mestu. Obdelava osebnih podatkov zaposlenih je dopustna le, če je to nujno za izpolnjevanje zakonskih obveznosti delodajalca ali za uresničevanje zakonitega interesa, pri čemer morajo biti spoštovana načela sorazmernosti in najmanjšega obsega podatkov.

ZVOP-2 v 78. členu določa, da je izvajanje videonadzora na delovnem mestu dopustno le v izjemnih primerih, kadar z drugimi ukrepi ni mogoče doseči varnostnega cilja. Poleg tega:

- snemanje ne sme biti usmerjeno neposredno v delovna mesta,
- zaposleni morajo biti predhodno obveščeni o videonadzoru (ZVOP-2, 2022, člen 77),
- stalni nadzor zaposlenih ni dopusten (npr. spremljanje vsakega njihovega gibanja),

- izvajalec mora izkazati, da so koristi nadzora večje od vpliva na pravice posameznika (načelo tehtanja interesov).

- **Primeri v praksi**

Tipične oblike nadzora zaposlenih vključujejo:

- videonadzor vhodov in izhodov iz poslovnih prostorov,
- nadzor gibanja po varovanih območjih,
- evidenco prihodov in odhodov z delovnega mesta (npr. sezam kartice),
- spremljanje uporabe službene opreme.

V vseh primerih mora biti obdelava nujna za zakonit namen, ustrezno dokumentirana in vključevati omejeno hrambo podatkov (npr. 1 leto pri videonadzoru, ZVOP-2, člen 76).

3.5.2 Nadzor obiskovalcev

Tudi nadzor obiskovalcev, npr. v poslovnih, turističnih ali industrijskih objektih, predstavlja obdelavo osebnih podatkov. Najpogostejše oblike vključujejo:

- evidence obiskovalcev, v katere se vpišejo ime, priimek, čas prihoda in odhoda, podjetje ali namen obiska,
- izdaja začasnih identifikacijskih kartic (t. i. sezam kartice),
- videonadzor skupnih prostorov (vhodi, hodniki, dvigala).

Zahteve po zakonitosti

Obdelava podatkov obiskovalcev mora temeljiti na zakonitem interesu varovanja ljudi in premoženja (GDPR, člen 6(1)(f)), vendar mora upravljavec:

- posameznike jasno informirati o obdelavi (GDPR, člen 13),
- omejiti obseg podatkov na nujno potrebne (npr. ne zbirati EMŠO ali drugih občutljivih podatkov),
- določiti rok hrambe (npr. izbris evidence po določenem času).

Informacijski pooblaščenec priporoča, da so evidence obiskovalcev:

- elektronske ali fizično varovane,
- nedostopne tretjim osebam,
- vodene na način, da ne razkrivajo podatkov predhodnih obiskovalcev.

Sorazmernost in transparentnost

Pomembno je, da izvajalci varovanja ne uporabljajo nadzora kot splošnega preventivnega ukrepa, temveč le v primerih, ko obstaja konkretna potreba (npr. vstop v območje z omejenim dostopom, zaščita občutljivih informacij, varovanja ljudi in premoženja).

Pri tem mora biti označen videonadzor na vstopnih točkah, jasno naveden upravljavec in kontakt za uveljavljanje pravic posameznika, kot zahtevata člen 13 GDPR (2016) in člen 76 ZVOP-2 (2022).

4 EVIDENTIRANJE IN OBDELAVA OSEBNIH PODATKOV V PODJETJU HIT D. D. NOVA GORICA

V tem poglavju predstavljam obdelavo osebnih podatkov z vidika lastnih izkušenj, ki sem jih pridobil kot skupinovodja varnostnikov v podjetju Hit d. d. Namen poglavja je prikazati konkretno izvajanje določb GDPR in ZVOP-2 v praksi, zlasti pri izvajanju videonadzora, vodenju evidenc in komunikaciji z zaposlenimi glede varstva osebnih podatkov (GDPR, 2016; ZVOP-2, 2022).

4.1 Predstavitev podjetja Hit d. d. in njegove varnostne službe

Podjetje Hit d. d. Nova Gorica je eno vodilnih igralniških in zabaviščnih podjetij v Sloveniji in širši regiji. Z več kot štiridesetimi leti izkušenj se je uveljavilo kot ključni deležnik na področju igralništva, gostinstva in turizma. Podjetje upravlja več znanih destinacij, kot so Perla Resort, Park Casino & Hotel, Mond Casino & Hotel, Korona Casino & Hotel in druge lokacije po vsej Sloveniji. Hit d. d. se ponaša z vrhunsko ponudbo igralniških storitev, luksuznimi namestitvami, gastronomijo ter širokim naborom zabavnih dogodkov, ob čemer stremi k odgovornemu igranju in trajnostnemu razvoju.

Kot skupinovodja varnostnikov v podjetju iz prve roke poznam pomen učinkovitega varnostnega sistema za zagotavljanje varnega okolja tako za goste kot za zaposlene. V podjetju Hit d. d. ima varnostna služba pomembno vlogo pri nemotenem poslovanju, saj skrbi za fizično in tehnično varovanje igralnic, hotelov, restavracij in spremljajočih objektov.

4.1.1 Naloge varnostne službe v kontekstu obdelave osebnih podatkov

Naše naloge vključujejo:

- nadzor nad vstopom v igralnice,
- stalno spremljanje dogajanja preko videonadzornega sistema, kar pomeni obdelavo osebnih podatkov obiskovalcev in zaposlenih,
- vodenje evidenc varnostnih dogodkov, evidenc škodnih primerov, pritožb ipd., ki prav tako vsebujejo osebne podatke,
- odziv na varnostne incidente in sodelovanje z državnimi organi v primeru suma kaznivih dejanj ali resnih kršitev.

Vsi ti postopki so povezani z obdelavo osebnih podatkov in so zato podvrženi določbam GDPR in ZVOP-2. Zavedamo se, da mora biti vsaka obdelava podatkov zakonita, sorazmerna in časovno omejena (GDPR, člen 5; ZVOP-2, členi 76–80).

4.1.2 Tehnično in organizacijsko varovanje podatkov

Podjetje Hit d. d. poleg fizične prisotnosti varnostnikov zagotavlja varnost osebnih podatkov tudi z naprednimi tehničnimi in organizacijskimi ukrepi. Ti vključujejo več medsebojno povezanih varnostnih sistemov:

- Sistem videonadzora je nameščen v igralniških prostorih, na hodnikih, vhodih in drugih skupnih površinah. Videoposnetki lahko vsebujejo osebne podatke posameznikov (slika, gibanje, vedenje), zato so ustrezno zaščiteni. Do sistema lahko dostopajo le pooblaščene osebe z individualnimi uporabniškimi računi in gesli. Prostor, kjer se nahaja strežniška oprema za videonadzor, je dodatno zavarovan s sistemom kontrole pristopa.
- Sistem kontrole dostopa omogoča spremljanje in omejevanje gibanja zaposlenih in obiskovalcev po posameznih območjih objekta glede na dodeljena pooblastila. Vsaka uporaba sistema je zabeležena digitalno, pri čemer mora vsak uporabnik za dostop do podatkov uporabiti svoje uporabniško ime in geslo. Tako se zagotavlja sledljivost in preprečuje nepooblaščen dostop.
- Protivlomni in protipožarni sistemi so integrirani z varnostno službo, kar omogoča takojšnje ukrepanje v primeru incidentov. Sistemi vključujejo zaznavanje gibanja, senzorje dima, panik tipke in druge zaščitne tehnologije. Povezani so z alarmnimi centri in omogočajo hitro odzivanje v nujnih primerih.

Z vsemi navedenimi tehničnimi in organizacijskimi ukrepi podjetje Hit d. d. zagotavlja, da so osebni podatki zaščiteni pred nepooblaščenim dostopom, izgubo ali zlorabo, skladno z zahtevami GDPR in ZVOP-2 (GDPR, 2016; ZVOP-2, 2022).

4.1.2.1 Interni pravilniki in varnostne politike podjetja Hit d. d.

Varstvo osebnih podatkov je v podjetju Hit d. d. obravnavano kot ena izmed temeljnih pravic in svoboščin posameznika, skladno z določbami Splošne uredbe o varstvu podatkov (GDPR, 2016) ter Zakona o varstvu osebnih podatkov (ZVOP-2, 2022).

Družba je sprejela več ključnih internih aktov, ki določajo pravila obdelave, zaščite in hrambe osebnih podatkov:

- Politika zasebnosti družbe Hit d. d. Nova Gorica,

- Pravilnik o varstvu in zavarovanju osebnih podatkov,
- Pogodba o obdelavi osebnih podatkov (za zunanje obdelovalce),
- Izjava o varstvu osebnih podatkov za zaposlene,
- Privolitev v obdelavo osebnih podatkov (osebna izjava zaposlenega).

Skladno s pravilnikom morajo vsi zaposleni pri svojem delu ravnati v skladu z načeli zakonitosti, poštenosti in preglednosti ter izvajati predpisane tehnične in organizacijske ukrepe za preprečitev nepooblaščenega dostopa, izgube ali zlorabe podatkov.

Del teh ukrepov predstavlja tudi politika varovanja gesel. Zaposleni so dolžni gesla za dostop do službenih sistemov redno menjati (najmanj na šest mesecev) ter upoštevati naslednje varnostne zahteve:

- minimalna dolžina gesla: 10 znakov,
- uporaba velikih in malih črk, številk ali posebnih znakov,
- prepoved uporabe šumnikov in osebnih podatkov (ime, priimek),
- razlika od zadnjih desetih uporabljenih gesel,
- zakasnitev najmanj deset dni med dvema spremembama gesla.

Takšen pristop k varstvu osebnih podatkov dokazuje, da podjetje sistematično izvaja varnostne politike in s tem krepi skladnost s predpisi ter zmanjšuje tveganja pri obdelavi podatkov (Hit d. d., b. d.).

4.1.3 Skladnost s pravnim okvirom

Vsi varnostni postopki temeljijo na:

- zakonitem interesu za zaščito ljudi in premoženja (GDPR, člen 6(1)(f)),
- zakonski obveznosti izvajalca zasebnega varovanja, določeni z ZVOP-2 (2022) in ZZasV-1 (2011),
- internih aktih podjetja, ki določajo obseg, namen in način obdelave podatkov.

Zaradi narave dela je varnostna služba podučena s področja varstva osebnih podatkov, predvsem v povezavi z uporabo kamer, postopki identifikacije, zahtevki za dostop do podatkov in zaščito informacij pri komunikaciji z gosti.

S tem Hit d. d. ne zagotavlja zgolj fizične varnosti, temveč tudi zakonito in odgovorno obdelavo osebnih podatkov, kar je nujen pogoj za poslovanje v igralniški panogi in za spoštovanje pravic vseh vključenih posameznikov.

4.2 Evidentiranje in obdelava osebnih podatkov pri opravljanju varnostnih storitev

V podjetju se pri izvajanju varnostnih storitev dnevno srečujemo z različnimi oblikami obdelave osebnih podatkov, ki so povezane z varnostnimi dogodki, videonadzorom površin v lasti podjetja, varovanjem premoženja ter upravljanjem dostopov do prostorov. Kot ena izmed odgovornih oseb za varnost aktivno sodelujem pri izvajanju teh postopkov, zato lahko neposredno potrdim, da je skladnost z zakonodajo vsakodnevna skrb našega operativnega delovanja.

4.2.1 Vrste evidenc in njihova zakonitost

V okviru dejavnosti zasebnega varovanja se za zagotavljanje varnosti postopkov in skladnosti z zakonodajo vodi več vrst evidenc, ki vsebujejo osebne podatke. V nadaljevanju so opisane najpogostejše evidence, ki jih vzdržuje varnostna služba podjetja Hit d. d.:

- **Evidenca izdanih sezam kartic**
  Omogoča nadzor nad izdajo in uporabo osebnih identifikacijskih kartic (sezam kartic), ki se uporabljajo za dostop do določenih varovanih območij. Zajema podatke o imenu in priimku uporabnika, datumu rojstva, datumu izdaje in preklica kartice, ravni dostopa ter odgovorni osebi za izdajo. Namen evidence je zagotavljanje sledljivosti dostopov ter preprečevanje nepooblaščenega gibanja po območjih z omejenim dostopom.
- **Evidenca varnostnih dogodkov**
  Vključuje zapise o vseh pomembnejših varnostnih incidentih, posredovanjih varnostnikov, zaznanih kršitvah in drugih dogodkih, ki so relevantni za zagotavljanje varnosti. V evidenci se lahko beležijo podatki o udeleženih osebah (ime, priimek, kontaktni podatki, datum rojstva, prebivališče, naziv sedeža imetnika licence), opisu dogodka, času in kraju ter ukrepih, ki so bili sprejeti. Evidenca služi kot pomembno orodje za analizo tveganj in pripravo nadaljnjih preventivnih ukrepov.
- **Evidenca dostopov do videoposnetkov**
  Vodi se skladno s 30. členom GDPR z namenom zagotavljanja revizijske sledljivosti. Beleži se, kdo je dostopal do posameznih videoposnetkov, kdaj, zakaj ter katere posnetke je pregledoval ali izvažal. S tem se zagotavlja nadzor nad uporabo občutljivih podatkov in preprečuje njihova zloraba (GDPR, 2016).
- **Evidenca izdanih depo trezorjev**

Vodi se za primere, ko gostje najamejo sef za varno shranjevanje osebnih predmetov. Evidenca zajema osebne podatke najemnika (ime, priimek, številka osebnega dokumenta), številko dodeljenega sefa, številko pogodbe ter čas najema in vračila. Podatki se obdelujejo za namen varnosti in zagotavljanje sledljivosti.

- **Evidenca najdenih predmetov**
  Namenjena je beleženju najdenih osebnih predmetov, ki jih obiskovalci pomotoma pustijo na varovanih površinah. Evidenca vključuje opis najdenega predmeta, lokacijo in čas najdbe, podatke o osebi, ki je predmet našla ali prevzela, ter postopke vračila lastniku. S tem se zagotavlja odgovorno in transparentno ravnanje z izgubljenimi predmeti.
- **Evidenca zapisnikov o poškodovanju osebnih predmetov**
  V tej evidenci se evidentirajo primeri, ko pride do poškodovanja lastnine oseb na območju podjetja (npr. vozil na parkirišču, osebne prtljage ali drugega premoženja). Evidenca vključuje opis dogodka, podatke o vpletenih osebah, okoliščinah poškodbe ter sprejetih ukrepih. Namen je omogočiti nadaljnje reševanje zahtevkov, zavarovalniških postopkov in zagotavljanje pravne zaščite podjetja.
- **Evidenca o nudenju prve medicinske pomoči**
  Zajema primere, ko varnostno ali drugo usposobljeno osebje nudi prvo pomoč na območju podjetja. Evidenca vključuje podatke o poškodovani osebi, datum rojstva, prebivališče, ime in priimek osebe, ki je prvo pomoč nudila, opis poškodbe, čas in kraj dogodka ter vrsto oskrbe. Namen evidence je zagotavljanje varnosti in zaščite zdravja ljudi ter dokumentiranje primerov za nadaljnjo presojo (npr. v pravnih postopkih).

Obdelava teh podatkov temelji na zakonitem interesu podjetja za zagotavljanje varnosti ljudi in premoženja ter na zakonski obveznosti izvajanja zasebnega varovanja (ZVOP-2, členi 76–77).

Pri tem vedno upoštevamo načela omejitve namena, minimizacije podatkov in časovne omejitve hrambe, kot jih določa člen 5 GDPR (2016).

4.2.2 Varnostni ukrepi in dostop do evidenc

V podjetju Hit d. d. je varovanje osebnih podatkov zasnovano celovito, saj se kombinirajo fizični, tehnični in organizacijski ukrepi. Evidenca varnostnega osebja je shranjena v posebej varovanih prostorih z nadzorovanim dostopom, kjer je fizična dokumentacija zaklenjena, elektronski zapisi pa so zaščiteni z gesli in dostopni le pooblaščenim osebam. Enako strogo je urejen dostop do videoposnetkov, ki ga ima izključno pooblaščeno varnostno osebje. Vsak

vpogled v posnetke se natančno beleži tako v elektronskem sistemu kot tudi v fizično vodeni knjigi videonadzornega sistema, kar zagotavlja popolno sledljivost.

Varnostni dogodki, obvestila in zapisi o incidentih se vodijo na interni ravni v kombinirani obliki – deloma elektronsko in deloma fizično, pri čemer so vse evidence shranjene v prostorih s strogo kontrolo dostopa. Posebno pozornost namenjamo tudi usposabljanju zaposlenih.

Notranji akti podjetja jasno določajo roke hrambe posameznih evidenc, ki so praviloma omejeni na največ pet let. V primerih, ko zakonodaja zahteva daljše obdobje ali ko podatki predstavljajo del uradne preiskave, se hramba lahko podaljša do zaključka postopkov. Takšen sistem varovanja zagotavlja skladnost z zakonodajo, preprečuje nepooblaščene dostope in krepi zaupanje v odgovorno ravnanje podjetja s podatki posameznikov.

4.2.3 Operativni postopki in odgovornosti

V okviru svojih nalog v varnostni službi sem med drugim odgovoren za zagotavljanje pravilnega vodenja evidenc, ki vsebujejo osebne podatke, ter za poročanje o vseh incidentih, kjer bi lahko prišlo do posega v pravice posameznikov. Tesno sodelujem z vodjo varnostne službe, notranjo revizijo in pooblaščeno osebo za varstvo podatkov (DPO) pri ocenjevanju tveganj, povezanih z obdelavo osebnih podatkov, zlasti v primerih, kjer so prisotne posebne okoliščine ali občutljive informacije.

Pomemben del mojega dela je tudi podpora pri obravnavi zahtev za dostop do osebnih podatkov s strani posameznikov, kar vključuje pomoč pri zbiranju in pripravi informacij v skladu z določili 15. člena GDPR. Poleg tega skrbim za pravočasno brisanje osebnih podatkov, ko potečejo zakonski ali interni roki hrambe (GDPR, 2016).

Delo varnostne službe se redno preverja s strani notranjih revizork, ki ocenjujejo skladnost postopkov z notranjimi akti in zakonodajo. Po potrebi lahko nadzor opravi tudi nadzorni organ, ki ima na osnovi 26. do 29. člena ZVOP-2 pooblastila za izvajanje inšpekcijskega nadzora (ZVOP-2, 2022).

4.2.4 Izzivi pri vsakodnevnem delu

Kljub jasno določenim internim postopkom ter dobro vzpostavljenemu sistemu varovanja osebnih podatkov se pri vsakodnevnem delu v praksi še vedno srečujemo z določenimi izzivi. Pogosto prihaja do dvomov, ali je posamezna obdelava podatkov, kot je npr. beleženje registrskih številk ali obdelava določenih informacij obiskovalcev, skladna z zakonodajo. V

zadnjem času se pojavlja tudi vse več pobud za uporabo biometričnih sistemov za identifikacijo zaposlenih ali gostov, kar zahteva posebno previdnost in presojo dopustnosti takšnih rešitev.

Zelo občutljiv in hkrati kompleksen izziv ostaja pravica posameznikov do dostopa do podatkov oziroma do izbrisa, zlasti ko gre za posnetke videonadzora. Tehnična izvedba takšnih zahtev pogosto ni preprosta, saj obstaja tveganje, da bi ob tem posegli v zasebnost drugih oseb, ki se nahajajo na istem posnetku. V ta namen imamo v podjetju programsko opremo, ki omogoča zameglitev oseb in osebnih podatkov, do katerih prosilec ni upravičen.

Vse bolj pomembno je tudi ozaveščanje zaposlenih in gostov o pravicah, ki jih imajo. V praksi se še vedno dogaja, da zaposleni v podjetju ali gostje od varnostne službe pričakujejo posredovanje podatkov brez zadostne pravne podlage. Takšna pričakovanja moramo kot varnostno osebje vedno odločno zavrniti in hkrati razložiti zakonske okvire. V zadnjih mesecih smo temeljito pregledali in ustrezno dopolnili vse evidence, povezane z obdelavo osebnih podatkov, kar vključuje tudi pregled rokov hrambe in dostopov. Posebno pozornost smo namenili obvestilom za obiskovalce, zlasti v zvezi z videonadzorom, saj je prav to področje pogosto vir vprašanj in zahtev po pojasnilih. Prenovljeni so bili tudi notranji obrazci in postopki, ki se uporabljajo ob obdelavi podatkov (izdaja ključev, sezam kartic …), tako da bolj dosledno upoštevajo načela zakonitosti, sorazmernosti in preglednosti. Namen vseh teh sprememb je bil zagotoviti večjo pravno varnost tako za podjetje kot tudi za posameznike, katerih podatki se obdelujejo.

4.3 Uporaba video nadzora v praksi (tehnični in organizacijski vidiki)

Videonadzor v podjetju predstavlja enega izmed temeljnih elementov celovitega sistema varovanja, saj bistveno prispeva k zagotavljanju varnosti oseb, varovanju premoženja ter nemotenemu delovanju igralniških dejavnosti. Zaradi posebnosti okolja, kjer poteka igralništvo – torej velikega števila dnevnih obiskovalcev ter manipulacije z gotovino in drugimi vrednostmi – je stalno spremljanje dogajanja znotraj in v okolici objektov nujno, tako z vidika preventivnega delovanja kot tudi kasnejše obravnave morebitnih incidentov.

V svoji vlogi sem neposredno vključen v nadzor nad pravilnim delovanjem videonadzornega sistema. Moja odgovornost je, da skupaj z ostalimi člani varnostne službe skrbim za to, da je sistem neprekinjeno tehnično brezhiben, dostopen le pooblaščenim osebam in da se obdelava posnetkov izvaja v skladu z veljavno zakonodajo, zlasti določbami uredbe GDPR in Zakona o varstvu osebnih podatkov (ZVOP-2, 2022; GDPR, 2016).

4.3.1 Namen in obseg videonadzora

Videonadzorni sistem je zasnovan kot ključni del varnostne infrastrukture, katerega namen je zagotavljanje celovitega nadzora nad območji, kjer obstaja povečano tveganje za varnost oseb in premoženja. Videonadzor se izvaja na lokacijah, ki so z vidika poslovanja in varnosti posebej izpostavljene. Sem sodijo vhodni in izhodni prostori igralnic in hotelov, igralniški prostori, območja blagajn, prireditveni prostori, hodniki, skladišča, parkirišča in dostopne poti. Na teh mestih videonadzor pripomore k učinkovitemu preprečevanju kaznivih dejanj, nadzoru nad spoštovanjem hišnega reda, prepoznavanju varnostnih tveganj in kasnejši analizi morebitnih incidentov. Snemanje se ne izvaja v prostorih, kjer bi lahko prišlo do čezmernega posega v zasebnost posameznikov (sanitarije, hotelske sobe, dvigala ali garderobe). Takšna ureditev je skladna z določbami čl. 76 ZVOP-2, ki določa prepoved izvajanja videonadzora na mestih, kjer bi bil ta nesorazmeren z upravičenimi cilji obdelave. Namen snemanja je izključno zagotavljanje varnosti oseb in premoženja ter podpora pri izvajanju nalog, ki jih varnostna služba opravlja v okviru svojih pooblastil in odgovornosti.

4.3.2 Pravna podlaga in skladnost z zakonodajo

Obdelava videoposnetkov v podjetju temelji na zakonitem interesu po zagotavljanju varnosti zaposlenih in obiskovalcev. Hkrati se pri izvajanju videonadzora upoštevajo določila Zakona o varstvu osebnih podatkov (ZVOP-2), zlasti členi od 76 do 80, ki natančno določajo pogoje in omejitve za zakonito uporabo videonadzornih sistemov v Sloveniji (ZVOP-2, 2022).

Vse površine, kjer se izvaja videonadzor, so ustrezno in jasno označene. Obvestila vsebujejo ključne informacije, kot so naziv in kontaktni podatki upravljavca, pravna podlaga za snemanje, namen obdelave ter kontaktna točka za pooblaščeno osebo za varstvo podatkov. Na ta način poskrbimo, da so posamezniki obveščeni o obstoju snemanja in svojih pravicah.

4.3.3 Tehnična zasnova sistema

Videonadzorni sistem, vzpostavljen v podjetju Hit d. d., je tehnično dovršen in zasnovan tako, da omogoča učinkovit nadzor nad dogajanjem na vseh ključnih lokacijah poslovanja. Sistem vključuje več sto visoko ločljivostnih IP-kamer, strateško nameščenih na varnostno občutljivih območjih, ki sem jih navedel že v poglavju 4.3.1. Zasnova sistema omogoča tako lokalni nadzor kot centralizirano spremljanje, kar pripomore k hitremu odzivanju na varnostne dogodke.

Nadzorni centri delujejo neprekinjeno 24 ur na dan in so pod nadzorom usposobljenega varnostnega osebja. Na posameznih lokacijah so nameščene lokalne snemalne enote, ki so

fizično in programsko zaščitene pred nepooblaščenim dostopom. Posnetki se digitalno arhivirajo in hranijo največ 30 dni, razen v primerih, ko so izločeni zaradi potrebe po preiskavi konkretnega dogodka ali kot dokazno gradivo v sodnem ali drugem uradnem postopku.

Posebna pozornost je namenjena sledljivosti dostopov do posnetkov. Vsak vpogled v videonadzorne posnetke se zabeleži tako v elektronskem sistemu kot tudi v fizični evidenci, ki se vodi ločeno in zagotavlja visoko stopnjo preglednosti ter odgovornosti pri obdelavi osebnih podatkov. S tem se preprečuje zloraba sistema in zagotavlja spoštovanje temeljnih načel varstva podatkov, kot so zakonitost, sorazmernost in preglednost.

4.4 Izkušnje zaposlenih glede spoštovanja GDPR pri vsakodnevnem delu

Skladnost z uredbo GDPR in Zakonom o varstvu osebnih podatkov (ZVOP-2) je za varnostno službo podjetja Hit d. d. del vsakodnevnega dela. Ker sem pri svojem delu nenehno v stiku z vprašanji, povezanimi z obdelavo osebnih podatkov, lahko z gotovostjo rečem, da so ta pravila in zahteve postali sestavni del naše prakse. Zaposleni jih ne dojemamo kot oviro, temveč kot pomemben del odgovornega ravnanja z informacijami posameznikov. Velik poudarek dajemo pravilni obdelavi in zaščiti podatkov, saj se zavedamo, da gre za občutljive vsebine, s katerimi je treba ravnati preudarno in skrbno. Iz izkušenj lahko potrdim, da so sodelavci v varnostni službi dobro seznanjeni s svojimi dolžnostmi, kar se kaže v doslednem spoštovanju internih pravil in zakonodaje (GDPR, 2016; ZVOP-2, 2022).

4.4.1 Raven ozaveščenosti zaposlenih

Varnostniki so dobro seznanjeni z osnovnimi določili, ki se nanašajo na:

- obveznost zaupnosti pri delu s podatki,
- pomen videonadzora in omejitve njegove uporabe,
- dolžnost informiranja obiskovalcev, da so prostori nadzorovani,
- postopke za vodenje evidenc obiskovalcev in izdajo sezam kartic.

Zaposleni se zavedajo, da se vsi zbrani podatki lahko obravnavajo kot osebni podatki in da mora biti njihova obdelava v skladu z načelom zakonitosti, sorazmernosti in omejitve namena (GDPR, člen 5).

Kljub temu so v praksi opažene tudi določene razlike v razumevanju, zlasti med mlajšimi in starejšimi varnostniki, kar kaže na potrebo po rednem usposabljanju.

4.4.2 Pogoste dileme in težave v praksi

a) Zahteve za ogled videoposnetkov

Pogost primer je, ko gost ali zaposleni zahteva ogled videoposnetkov, na katerih se nahaja tudi več drugih oseb. V takih primerih moramo kot varnostniki odkloniti neposredni ogled, saj bi s tem kršili zasebnost tretjih oseb (ZVOP-2, člen 80; GDPR, člen 15). Namesto tega predlagamo uradno zahtevo po izvodu določenega dela posnetka, o kateri odloča vodstvo varnostne službe v sodelovanju s pooblaščeno osebo za varstvo podatkov (GDPR, 2016; ZVOP-2, 2022).

b) Vodenje evidenc

V preteklosti se je v evidenco ukrepov varnostnika zapisovalo več podatkov, kot je bilo potrebno (npr. EMŠO), kar ni v skladu z načelom minimizacije podatkov (GDPR, člen 5(1)(c)). Po dodatnih navodilih in pojasnilih je bila praksa popravljena in zdaj zapisujemo le osnovne identifikacijske podatke (GDPR, 2016).

c) Nejasnosti pri hrambi podatkov

Ena od ponavljajočih se dilem je bila povezana z roki hrambe podatkov. Pri nekaterih evidencah smo zaposleni zmotno menili, da je podatke treba hraniti »za vsak primer« več mesecev. V skladu z določbami ZVOP-2 (člen 80) pa velja splošno pravilo, da je najdaljši rok za hrambo videoposnetkov šest mesecev, če ni konkretnega razloga za daljše hranjenje (ZVOP-2, 2022).

4.4.3 Notranje usposabljanje in izboljšave

V zadnjem letu je bila v podjetju Hit d. d. na pobudo notranje revizorke izvedena poglobljena presoja vodenja varnostnih evidenc, zlasti tistih, ki vključujejo obdelavo osebnih podatkov. Revizija je pokazala neusklajenosti glede obsega podatkov ter nedorečenih rokov hrambe. Na osnovi revizijskih ugotovitev so vodje varnosti skupaj s pravno službo pristopili k poenotenju in formalizaciji:

- vsebin in oblik evidenc (npr. posredovanja, dostopi do videoposnetkov),
- delovnih navodil,
- postopkov za izbris oziroma anonimizacijo podatkov,
- protokolov za vpogled v podatke in odgovor na zahteve posameznikov (npr. po členu 15 GDPR) (GDPR, 2016).

Ta pobuda je bistveno pripomogla k izboljšanju pravne skladnosti, zmanjšanju tveganj za kršitev zakonodaje in dvigu ozaveščenosti sodelujočega varnostnega osebja, ki je zdaj bolj samozavestno pri delu z evidencami in zahtevami posameznikov.

4.4.4 Odnos zaposlenih do varstva podatkov

Med zaposlenimi je opaziti vse večje zavedanje, da varstvo osebnih podatkov ni zgolj zakonska zahteva, temveč tudi pomemben del strokovne etike in osebne integritete. Posebej v varnostni službi, kjer zaposleni vsakodnevno obravnavajo občutljive informacije, postaja pravilno ravnanje s podatki temelj zaupanja, ki ga podjetje gradi tako znotraj kolektiva kot tudi z gosti.

Večina varnostnikov se dobro zaveda, da lahko nepazljivo ali neustrezno ravnanje s podatki ogrozi ugled podjetja, načne zaupanje obiskovalcev in pripelje do strožjih posledic, kot so upravne kazni, določene v Splošni uredbi o varstvu podatkov. Prav zato večina zaposlenih z veliko odgovornostjo pristopa k nalogam, povezanih z obdelavo osebnih podatkov, in upošteva tako interne akte kot zakonske določbe.

Kljub temu obstaja prostor za nadgradnjo praktičnega znanja. Zaposleni bi si želeli več vsebin, ki presegajo osnovno teoretično poznavanje predpisov – na primer konkretne napotke in usmeritve za ravnanje v specifičnih situacijah, kot so obravnava zahteve za izbris podatkov, postopek ob gostu, ki zahteva kopijo videoposnetka, ali pravilno ukrepanje ob incidentu, kjer je prišlo do razkritja osebnih podatkov. Takšne praktične vsebine bi dodatno okrepile samozavest zaposlenih in izboljšale odzivnost v občutljivih okoliščinah, kar je v hitro spreminjajočem se delovnem okolju izjemno pomembno.

5 PRAKTIČNI IZZIVI IN ANALIZE

V tem poglavju analiziram dejansko stanje obdelave osebnih podatkov v podjetju Hit d. d. z vidika vsakodnevnega izvajanja varnostnih nalog. Analiza temelji na lastnih izkušnjah, notranjih postopkih, usmeritvah varnostne službe ter zakonskih zahtevah. Cilj je prepoznati izzive pri zagotavljanju skladnosti z GDPR in ZVOP-2, izpostaviti pomanjkljivosti ter jih primerjati s priporočili Informacijskega pooblaščenca (GDPR, 2016; ZVOP-2, 2022).

5.1 Skladnost obdelave podatkov z GDPR in ZVOP-2 v podjetju Hit d. d.

Podjetje Hit d. d. si na področju varstva osebnih podatkov prizadeva ne le za formalno skladnost z zakonodajo, temveč tudi za vzpostavitev visoke ravni odgovorne prakse. Skladnost z določili Splošne uredbe o varstvu podatkov (GDPR) in Zakona o varstvu osebnih podatkov (ZVOP-2) se v podjetju odraža v več vidikih delovanja. Prostori, kjer se izvaja videonadzor, so jasno in ustrezno označeni, kar posameznikom omogoča, da se zavedajo svojih pravic in obsega nadzora. Hkrati so informacije o upravljavcu, namenu snemanja in pravni podlagi ustrezno prikazane, kot to zahtevata člen 13 GDPR (2016) in člen 76 ZVOP-2 (2022).



Slika 1: Obvestilo o izvajanju video nadzora v podjetju Hit d. d.

Vir: (Hit d. d., b. d.)

Ureditev hrambe posnetkov je skladna z zakonodajo, saj se ti praviloma hranijo največ 30 dni, razen v primerih, ko so potrebni kot dokaz v postopku ali na osnovi zahteve pristojnih organov. Dostopi do videoposnetkov in evidenc dejavnosti obdelave so natančno beleženi, kar zagotavlja sledljivost in omogoča revizijski nadzor nad ravnanjem z osebnimi podatki.

Zaznati je tudi pozitiven premik v zavedanju zaposlenih o pomembnosti varstva osebnih podatkov. Ta premik ni posledica zgolj internih pravil ali pravnih zahtev, temveč tudi strokovnega vodenja varnostne službe in rednega nadzora notranje revizije, ki z občasnimi pregledi prispeva k stalnemu izboljševanju praks. Takšen celosten pristop ustvarja stabilno okolje, v katerem je varstvo podatkov sestavni del organizacijske kulture.

5.2 Ugotovljene pomanjkljivosti in tveganja

Kljub dobrim temeljem smo v praksi zaznali več izzivov in odprtih vprašanj, ki kažejo na potrebo po dodatnem izboljšanju:

5.2.1 Neenotna praksa vodenja evidenc

Pred revizijo smo po različnih enotah uporabljali različne obrazce in postopke (npr. najdeni predmeti, evidence izdaje ključev in sezam kartic). To je povzročilo nepreglednost in povečalo tveganje za nenamensko obdelavo podatkov. Poenotenje dokumentacije je bilo izvedeno šele v zadnjem obdobju.

5.2.2 Dvomi pri obravnavi zahtev posameznikov

V praksi se zaposleni še vedno srečujejo z negotovostjo, kako obravnavati prošnje za ogled videoposnetkov ali zahteve za izbris podatkov. Ker so te vloge pogosto čustveno obarvane (npr. v primerih sporov med gosti), je pomembno, da varnostna služba ostane objektivna in zakonsko dosledna, kar pa zahteva jasno podporo vodstva.

5.2.3 Omejena tehnična zaščita pri nekaterih evidencah

Nekatere evidence, predvsem v fizični obliki, niso bile vedno ustrezno zaščitene (npr. z zaklepanjem v omare). Notranja revizija je to izpostavila kot potencialno točko tveganja, kar smo že rešili z digitalizacijo in omejitvijo dostopa po vlogah.

5.3 Primerjava s priporočili Informacijskega pooblaščenca

Informacijski pooblaščenec Republike Slovenije je v zadnjih letih izdal vrsto smernic in priporočil, ki predstavljajo pomembno izhodišče za zakonito in odgovorno ravnanje z osebnimi podatki. Poseben poudarek namenja področju videonadzora, kjer izpostavlja načelo sorazmernosti in obveznost jasnih označitev nadzorovanih območij. Prav tako opozarja na odgovorno obravnavo dostopa do osebnih podatkov, pri čemer je treba vedno tehtati pravice in

interese vseh vpletenih posameznikov. Na področju obdelave podatkov zaposlenih pa izrecno izpostavlja prepoved stalnega in nekontroliranega nadzora delovnega mesta, kot to določa 80. člen ZVOP-2 (2022).

Analiza stanja v podjetju kaže, da se v veliki meri držimo teh priporočil in da je ureditev v praksi večinoma skladna s pričakovanji nadzornega organa. Kljub temu obstajajo nekatera področja, kjer bi bilo mogoče obstoječe prakse še izboljšati. Ena izmed možnosti bi bila natančnejša opredelitev razmerja med upravljavci in obdelovalci podatkov, zlasti v primerih, ko vzdrževanje tehnične opreme izvajajo zunanji pogodbeni partnerji (videonadzor, kontrola pristopa).

Dodaten potencial za izboljšave se kaže tudi na področju komunikacije z zaposlenimi in obiskovalci. Bolj proaktivno in razumljivo informiranje o njihovih pravicah bi lahko dodatno okrepilo zaupanje in zmanjšalo možnosti za nesporazume. S tem bi podjetje še bolj utrdilo svoj ugled kot družba, ki varstvo osebnih podatkov obravnava resno in celovito.

6 PRIPOROČILA ZA IZBOLJŠAVO

Podjetje Hit d. d. ima na osnovi analize stanja in lastnih operativnih izkušenj sistem obdelave in varstva osebnih podatkov vzpostavljen na visoki ravni pravne in organizacijske skladnosti. Kljub temu pa lahko tudi odlično vzpostavljen sistem koristi ciljnim izboljšavam, ki pripomorejo k še večji učinkovitosti, preglednosti in odpornosti na nova tveganja.

6.1 Predlogi za izboljšanje skladnosti z zakonodajo

Obstoječi sistem varstva osebnih podatkov v podjetju Hit d. d. je skladen z zahtevami GDPR in ZVOP-2, kar potrjujejo tudi ugotovitve notranje revizije. Kljub temu obstajajo možnosti za manjše nadgradnje, ki bi dolgoročno pripomogle k ohranjanju visoke ravni skladnosti (GDPR, 2016; ZVOP-2, 2022).

Menim, da bi bilo koristno:

- združiti vse obstoječe interne akte in postopke varstva osebnih podatkov v enoten priročnik za zaposlene, ki bi bil preprosto dostopen in razumljiv ter bi ponujal jasna navodila, kako ravnati v določenih postopkih,
- uvesti preprost notranji kontrolni seznam (checklist), s katerim bi vodje oddelkov lahko občasno preverjali, ali se vsakodnevni postopki, kot so hramba evidenc, ustrezna označitev nadzorovanih prostorov in fizično varovanje dokumentacije, izvajajo skladno z zahtevami.

Predlagani ukrepi ne izhajajo iz zaznanih pomanjkljivosti, temveč iz želje po preventivni krepitvi sistema, ki bi zagotavljal stabilno in trajno skladnost tudi v primeru sprememb zakonodaje ali uvedbe novih tehnologij.

6.2 Izobraževanje zaposlenih in ozaveščanje

Čeprav je varnostna služba podjetja Hit d. d. na področju varovanja ljudi in premoženja zelo profesionalna in izkušena, do zdaj ni bilo izvedenih formalnih izobraževanj ali usposabljanj varnostnega osebja s področja varstva osebnih podatkov. Praksa in razumevanje določb GDPR ter ZVOP-2 sta se večinoma oblikovala skozi interno prenašanje znanja, individualno samoiniciativo in operativne izkušnje (GDPR, 2016; ZVOP-2, 2022).

Kot skupinovodja varnostnikov menim, da bi bilo smiselno v prihodnje razmisliti o uvedbi naslednjih oblik ozaveščanja zaposlenih:

- osnovno začetno usposabljanje za varnostno osebje, ki bi vključevalo osnove GDPR in ZVOP-2 (GDPR, 2016; ZVOP-2, 2022),
- kratki letni obnovitveni moduli v obliki elektronskega kviza ali praktičnega primera iz varnostne službe,
- notranja digitalna obvestila z opomniki glede odgovornega ravnanja z osebnimi podatki (npr. »Kaj narediti ob zahtevi za ogled videoposnetkov?«).

Tovrstna ozaveščanja ne bi bila zahtevna za izvedbo, predstavljala pa bi pomemben korak k formalizaciji znanja, zmanjševanju tveganj in dodatnemu utrjevanju kulture odgovorne obdelave osebnih podatkov.

6.3 Tehnične rešitve za večjo varnost podatkov

Varnost občutljivih podatkov, ki se prikazujejo na monitorjih, je mogoče dodatno izboljšati z uporabo tehnologij, ki omejujejo možnost nepooblaščenega vpogleda ali snemanja. Ena izmed preprostih in takoj izvedljivih rešitev je namestitev »privacy filtrov« na zaslone. Ti filtri fizično omejijo vidni kot tako, da je slika na zaslonu jasna le za osebo, ki gleda neposredno od spredaj, z bočnih strani pa je prikaz zatemnjen. Tak ukrep preprečuje, da bi mimoidoči opazili prikazane informacije, in je še posebej uporaben v pisarnah, kjer se na zaslonih obdelujejo osebni podatki, na delovnih pultih v igralnici, recepciji ipd.

Poleg te fizične zaščite se v prihodnje obeta tudi razvoj digitalnih rešitev, ki bi zaznale usmerjeno kamero telefona ali fotoaparata proti zaslonu in samodejno zameglile ali zatemnile prikaz. Čeprav ta tehnologija še ni komercialno dostopna, predstavlja zanimivo možnost za prihodnje izboljšave varovanja informacij. Vključitev takih funkcionalnosti bi lahko v kombinaciji s fizičnimi filtri zagotovila še višjo raven varnosti.

7 SKLEP

V diplomskem delu sem proučil vpliv Splošne uredbe o varstvu podatkov (GDPR) in nacionalnega Zakona o varstvu osebnih podatkov (ZVOP-2) na področje zasebnega varovanja s posebnim poudarkom na podjetju Hit d. d. Nova Gorica. Analiza je pokazala, da gre za področje, kjer se dejavnosti izvajalcev zasebnega varovanja močno prepletajo z obdelavo osebnih podatkov. To pomeni, da morajo podjetja v tej panogi ne le dosledno upoštevati veljavne predpise, temveč tudi vzpostaviti praktične in učinkovite rešitve, ki bodo zagotavljale ravnotežje med varnostnimi potrebami in varstvom pravic posameznikov.

Ključna spoznanja raziskave kažejo, da so osebni podatki sestavni del skoraj vseh procesov zasebnega varovanja: od videonadzora, vodenja evidenc ukrepov do uporabe sezam kartic in sistemov za identifikacijo oseb. Vsak od teh procesov odpira pomembna pravna in etična vprašanja, ki jih izvajalci varovanja ne morejo prezreti. Ravno zato GDPR in ZVOP-2 ne pomenita zgolj formalne obveznosti, temveč postavljata temelj za odgovorno, zakonito in transparentno obdelavo osebnih podatkov. V tem okviru se še posebej uveljavljajo načela, kot so sorazmernost, zakonitost, omejitev namena in časovne omejitve hrambe podatkov, ki usmerjajo izvajalce k bolj premišljenemu ravnanju.

Analiza primera podjetja Hit d. d. je pokazala, da ima to podjetje večino ključnih postopkov varstva osebnih podatkov ustrezno urejenih in usklajenih z zakonodajnimi zahtevami. Posebnost podjetja je v tem, da skladnost z zakonodajo razume kot del svoje širše poslovne kulture in odgovornosti do gostov, zaposlenih ter širše javnosti. Interna revizija, usklajevanja med oddelki in stalno izboljševanje procesov so v tem primeru pripomogli k temu, da je obdelava osebnih podatkov postala sestavni del kakovostnega in zanesljivega izvajanja varnostnih storitev. Takšna praksa kaže, da je mogoče zakonske zahteve ne le izpolnjevati, temveč jih razumeti kot priložnost za krepitev zaupanja in ugleda podjetja.

Pri preverjanju hipotez sem ugotovil, da številna varnostna podjetja še nimajo vzpostavljenih celovitih sistemov varstva osebnih podatkov, kar potrjuje, da panoga kot celota zaostaja za zakonodajnimi zahtevami. Hit d. d. pri tem izstopa kot dober primer prakse, saj kaže, kako lahko premišljeno upravljanje z osebnimi podatki prispeva k višji kakovosti storitev. Druga hipoteza, da je GDPR pomembno vplival na spremembe praks, se je v celoti potrdila – tako v skrajšanju rokov hrambe, označevanju nadzorovanih prostorov kot tudi pri zagotavljanju pravic posameznikov. Tretja hipoteza, ki se je nanašala na izzive videonadzora, je bila delno potrjena:

največ težav se v praksi pojavlja pri dokumentaciji in urejanju dostopa do posnetkov, medtem ko je tehnični vidik sistemov večinoma stabilen.

Pomemben vidik raziskave je bilo tudi povezovanje teoretičnih zahtev z mojimi praktičnimi izkušnjami z delovnega mesta skupinovodje v varnostni službi. Prav zaradi tega sem lahko predstavil realističen prikaz stanja na terenu, ki presega zgolj akademski okvir. Spoznal sem, da vloga varnostnega osebja obsega več kot fizično varovanje – vključuje tudi izjemno pomembno odgovornost pri obdelavi osebnih podatkov. To zahteva visoko raven pravne ozaveščenosti in odgovornosti, saj napačno ravnanje lahko pomeni poseg v temeljne pravice posameznikov in posledično škoduje tako podjetju kot celotni dejavnosti.

Raziskava je odprla tudi pomembna vprašanja za prihodnje delo in raziskovanje. Ena izmed ključnih usmeritev bi bila primerjalna analiza med različnimi izvajalci zasebnega varovanja, saj bi to omogočilo boljši vpogled v to, kako različno podjetja pristopajo k implementaciji zakonodaje. Nadalje se kot posebej aktualno kaže proučevanje vpliva biometričnih sistemov, ki predstavljajo nova tveganja za pravice posameznikov. Prav tako je pomembno analizirati učinkovitost internih usposabljanj, saj je ravno ozaveščeno in dobro usposobljeno varnostno osebje ključno za skladno obdelavo osebnih podatkov. Poleg tega bi bilo smiselno oceniti tudi vpliv priporočil informacijskega pooblaščenca na dejanske spremembe praks v panogi ter ugotoviti, v kolikšni meri ta priporočila prispevajo k večji skladnosti v praksi.

Sklepno lahko povzamem, da GDPR in ZVOP-2 predstavljata pomemben mejnik na področju zasebnega varovanja. Oba predpisa postavljata jasne zahteve, ki pa niso namenjene omejevanju dejavnosti, temveč zagotavljanju, da se varnost izvaja ob polnem spoštovanju človekovih pravic in dostojanstva posameznika. Učinkovito izvajanje teh predpisov v podjetju Hit d. d. dokazuje, da je skladnost mogoče doseči, če podjetje k temu pristopi sistematično, odgovorno in dolgoročno. Pričakovati je, da se bo pomen varstva osebnih podatkov v prihodnje še povečal, saj se tehnologije razvijajo, pričakovanja družbe naraščajo, pravice posameznikov pa se krepijo. Zato bo vloga varnostnega osebja v prihodnje vedno bolj usmerjena v združevanje strokovnega znanja s področja fizičnega varovanja in poznavanja pravnih zahtev na področju varstva osebnih podatkov.

8 LITERATURA

Hit d. d. (b. d.). *Politika zasebnosti.* Pridobljeno 20. avgusta 2025 s https://www.hit.si/politika-zasebnosti/

Informacijski pooblaščenec RS. (2023a, 26. januar). *Evidenca dejavnosti obdelave.* Pridobljeno s https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/ključna-področja-uredbe/evidenca-dejavnosti-obdelave

Informacijski pooblaščenec RS. (2023b, 15. december). *Smernice o uporabi piškotkov in podobnih sledilnih tehnologij.* Pridobljeno s https://www.ip-rs.si/publikacije/priročniki-in-smernice/smernice-po-splošni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-uporabi-piškotkov-in-podobnih-sledilnih-tehnologij

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) (GDPR). (2016). Uradi list EU, št. L119. Pridobljeno s https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32016R0679

Zakon o varstvu osebnih podatkov (ZVOP-1). (2007). Uradni list RS, št. 94/07 – uradno prečiščeno besedilo. Pridobljeno s https://www.uradni-list.si/1/content?id=79493

Zakon o varstvu osebnih podatkov (ZVOP-2). (2022). Uradni list RS, št. 163/22. Pridobljeno s https://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7959

Zakon o zasebnem varovanju (ZZasV-1). (2011). Uradni list RS, št. 17/11 s spremembami. Pridobljeno s https://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5760