

PRAVNI VIDIKI DIGITALIZACIJE V PODJETJIH

GAL PASTIRK

Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
gal.pastirk@student.um.si

Sinopsis Vsako podjetje si prizadeva postati čim uspešnejše in konkurenčnejše. V današnjih časih je te cilje nemogoče doseči, ne da bi se podjetje spoprijelo z izzivi digitalizacije. Digitalna preobrazba podjetij je tudi ena temeljnih idej EU, ki želi s tem okrepiti svoj položaj in izkoristiti sodobna znanja o digitalnih tehnologijah. Obenem pa se je ob tem neizogibno soočiti s pravnimi vprašanji, kot so nove oblike pogodbenih razmerij, varstvo osebnih podatkov in zasebnost na delovnem mestu, ki so posledice digitalne transformacije. Posamični primeri pravnega normiranja, nastalega kot posledica digitalizacije podjetniškega delovanja, so podkrepjeni s teorijo kot tudi s primeri prakse v dveh slovenskih podjetjih.

Ključne besede

pravni vidiki digitalizacije, računalništvo v oblaku, varstvu podatkov, informacijske rešitve, zasebnost na delovnem mestu

LEGAL ASPECTS OF DIGITALIZATION IN COMPANIES

GAL PASTIRK

University of Maribor, Faculty of Law, Maribor, Slovenia
gal.pastirk@student.um.si

Abstract Every company strives to become as successful and competitive as possible. Nowadays, it is impossible to achieve these goals without the company tackling the challenges of digitization. The digital transformation of companies is also one of the fundamental ideas of the EU, which wants to strengthen its position and take advantage of modern knowledge about digital technologies. At the same time, it is inevitable to face legal issues, such as new forms of contractual relationships, personal data protection and workplace privacy, which are the consequences of digital transformation. Individual examples of legal standardization, which arose as a result of the digitalization of business activities, are supported by theory as well as by examples of practice in two Slovenian companies.

Keywords:

legal aspects of
digitalization,
cloud computing,
data protection,
information
solutions,
privacy in the
workplace

1 Uvod

Digitalne tehnologije prinašajo veliko pozitivnih družbenih sprememb in se uporabljajo že skoraj v vseh gospodarskih sektorjih. Ob tem je treba pozornost nameniti tudi regulaciji novih tehnologij, ki se jih EU loteva previdno, a hkrati vseeno odločneje od drugih svetovnih velesil (Brkan, 2020). Pretirana regulacija v podjetjih bi lahko načela njihovo inovativnost, premalo le-te pa lahko pripelje do škodljivih posledic in kršitev temeljnih pravic. Tako gre pri pravni regulaciji digitalnih tehnologij za plutje med Scilo in Karibdo ter iskanje najprimernejših rešitev.

EU se zaveda, da evropsko gospodarstvo ne bo ostalo konkurenčno ameriškim in kitajskim rivalom, če ne bo prišlo do korenitih sprememb. Smer, ki jo je EU izbrala v času okrevanja po epidemiji, je smer zelene in digitalne prihodnosti. Odpornost, okrevanje in strateška avtonomija EU so v glavnem fokusu razvoja stare celine. To smer je čutiti tudi v podjetjih. Zavedajo se, da digitalne rešitve vodijo k večji konkurenčnosti, inovacijam in rasti evropskega gospodarstva (Lee, 2019).

Podjetji Talum d.d. in Comtron d.o.o., ki smo ju vzeli pod drobnogled, sta se že soočili s številnimi izzivi, ki jih je prinesla digitalizacija. V nadaljevanju bodo predstavljena različna področja, na katera je proces digitalizacije že vplival, pa tudi to, kako so se s tem soočili v omenjenih podjetjih.

Ta prispevek ima v nadaljevanju sedem poglavij. Prvemu, uvodnemu poglavju, sledi drugo poglavje, ki zajema zaščito in varovanje podatkov v podjetjih. V tretjem poglavju so predstavljena nova pogodbeno razmerja za urejanje storitev računalništva v oblaku. Četrto poglavje obravnava dileme glede varstva osebnih podatkov v podjetjih. Nadalje je v petem poglavju predstavljen trajnostni razvoj v podjetjih, v šestem poglavju pa zasebnost na delovnem mestu. Prispevek se zaključuje s sklepom v sedmem poglavju.

2 Zaščita in varovanje podatkov v podjetjih

Podjetje, v katerem osrednjo dejavnost predstavljajo poslovni informacijski sistemi, je dolžno poskrbeti za varnost teh sistemov in preprečiti morebitne zlorabe. Da so podatki, ki so hranjeni na strežnikih, najboljše zavarovani, je za osnovno varovanje potrebno dvoje: varna shramba in varnostno kopiranje podatkov.

V svetu so razmere, tudi zaradi novih tehnologij, postale nepredvidljive. Napredek na področju digitalizacije pomeni tudi rast kibernetских groženj. Kibernetски kriminalci so izkoristili pandemijo covid-19 in se še posebej osredotočajo na organizacije in podjetja (Evropski parlament, 2022).

Podoben primer nakazuje vojna v Ukrajini. Še preden so ruski tanki zavzeli dele Ukrajine, so bili priča kibernetским napadom po državi. Na drugi strani so hekerske skupine napovedale odkrito kibernetско vojno proti ruski administraciji.

V evropskem merilu omenjene težave naslavlja predlog Direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetiske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148, ki upošteva spremenjeno stanje na področju kibernetских groženj ter vpeljuje usklajene ukrepe širom EU, med njimi tudi zaščito ključnih sektorjev (Evropski parlament, 2022).

3 Nova pogodbena razmerja za urejanja storitev računalništva v oblaku

Med ključne kibernetiske grožnje, ki jih je že za časa pandemije prepoznala Evropska agencija za kibernetско varnost (angl. The European Union Agency for Cybersecurity), med drugim sodijo vdori v podatkovne sisteme (Evropski parlament, 2022). Izpostavljene kibernetiske grožnje in varnost podatkov pred vdori so relevantne tudi za srednje velika in velika podjetja, kot sta Comtron d.o.o. in Talum d.d.

Nadalje je treba zagotoviti ustrezno lokacijo shranjevanja podatkov, saj morajo strežniki zagotavljati ustrezno požarno in potresno varnost. Za podjetja, kot je Comtron d.o.o., so podatki ključni izdelek, ki ga je podjetje ustvarilo. Za varnost podatkov tudi zaradi njihovega obsega največkrat pride v poštev računalništvo v oblaku. V oblak se prenesejo podatki, za katere naročnik ne želi, da se razkrijejo, ki so zaupni in pri katerih se od ponudnika pričakuje, da jih ustrezno varuje (Andrejek, 2019).

Zaradi varnosti ima podjetje strežniško infrastrukturo urejeno na svoji lokaciji, to je v Comtronu d.o.o., in na Pošti Slovenije, kjer obstaja dodatna varnostna kopija podatkov (R. Jelen, osebna komunikacija, 12. 5. 2022). Pošta Slovenije je v procesu digitalne preobrazbe vzpostavila enega vodilnih zasebnih računalniških oblakov v

Sloveniji in regiji. Obenem je v svojih podatkovnih središčih vzpostavila tudi temeljne storitve za varno in zakonsko skladno digitalno poslovanje podjetij, javnih ustanov in prebivalcev. Storitve računalništva v oblaku, ki ga je vzpostavila Pošta Slovenije, danes najemajo številna podjetja z več kot desetimi zaposlenimi (Posel se seli, 2020).

Ker se struktura podjetij zaradi digitalne transformacije nenehno spreminja, so tudi potrebe, ki jih le-ta imajo, drugačne. Ena izmed ključnih je varno shranjevanje podatkov in zagotavljanje njihove varnostne kopije. Izvajanje glavne profitne dejavnosti je tako pogojeno z informacijsko tehnologijo, ki jo omogočajo storitve računalništva v oblaku.

Računalništvo v oblaku poslovnim uporabnikom omogoča shranjevanje podatkov in njihovo varno hrambo.

O splošni definiciji računalništva v oblaku zaenkrat še ne moremo govoriti. Lahko pa pojem za lažje razumevanje definiramo kot zagotavljanje računalniških zmogljivosti preko spletne povezave. Gre za najem zunanjih izvajalcev (outsourcing) na področju računalništva, kjer podjetje namesto izgradnje lastne infrastrukture in programske opreme le-to najame pri ponudniku storitev računalništva v oblaku (Andrejek, 2019).

Trg storitev računalništva v oblaku v EU je v porastu – med letoma 2019 in 2026 naj bi se vsako leto v povprečju povečal za dvanajst odstotkov (Posel se seli, 2020).

Temu primerno je sledilo tudi vse večje sklepanje pogodb o računalništvu v oblaku. K temu so pripomogle tudi fleksibilnost storitve in ugodne finančne posledice. Fleksibilnost predstavlja že kapaciteta oblaka, ki jo glede na svoje potrebe lahko prilagaja uporabnik. Obenem pa je povečanje zanimanja predvsem draga računalniška infrastruktura, ki se mora vzdrževati in posodabljati, s katero pa uporabnik nima težav, saj so to obveznosti ponudnika (Andrejek, 2019).

Pogodba o računalništvu v oblaku je pravni posel, ki pa ga Obligacijski zakonik (Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631), v nadaljevanju OZ, specifično ne ureja. Je ena izmed modernih pogodbenih tipov novejšega časa, ki pa ima elemente drugih (klasičnih) pogodb.

Vsebinsko je v veliki meri prepuščena volji ponudnika in naročnik le redko sodeluje pri njenem nastanku. Ponudnik s splošnimi pogoji pogodbe določi vsebino. V gospodarskem pogodbenem pravu se takšen tip pogodbe imenuje adhezijška pogodba. Stranki se pri takšnem tipu pogodbe o pogodbenih sestavinah praviloma ne dogovarjata, saj splošni pogoji pogodbe v celoti urejajo pogodbeno razmerje. Pravila obligacijskega prava pa so pri sklepanju pogodb preko splošnih pogojev strožja za tistega, ki je dotične splošne pogoje določil (120. člen OZ).

4 Dileme glede varstva osebnih podatkov v podjetjih

Prednostno skrb v zvezi s skladnostjo s slovensko zakonodajo pri računalništvu v oblaku je treba nameniti varstvu podatkov.

Intenzivni proces digitalizacije je povečal obseg zbiranja podatkov in pospešil pretok informacij o posameznikih. Ker je mogoče te podatke uporabiti v različne namene, je EU po več letih diskusije sprejela Splošno uredbo o varstvu podatkov 1 (angl. General Data Protection Regulation, GDPR, v nadaljevanju Splošna uredba) (Jamšek, 2018).

Zakon o varstvu osebnih podatkov (v nadaljevanju: ZVOP-1) ter predvsem Splošna uredba o varstvu podatkov določata nekaj razmerij, ki jih morata naročnik in ponudnik medsebojno urediti in upoštevati.

Predvsem je tukaj mišljena obdelava osebnih podatkov, ki je v današnjem digitalnem svetu bolj pravilo kot izjema – kadar koli subjekt obdeluje osebne podatke, pri tem deluje kot njihov upravljavec in obdelovalec (Lobo, 2020).

Sedanji zakonodajni okvir na področju varstva osebnih podatkov v EU je predvsem s Splošno uredbo sprožil niz vprašanj o njeni uporabi. Številne prakse podjetij so tako z 28. 5. 2018 postale neskladne z novo zakonodajo glede varstva osebnih podatkov. Mnoga vprašanja podjetnikov še danes ostajajo neodgovorjena, saj pristojni organi niso imeli dovolj časa, da bi v nacionalnem pravnem redu sprejeli ustrezne izvedbene ukrepe iz Splošne uredbe. Slednjemu smo priča tudi v Sloveniji (Pirc Musar idr., 2020).

Podobne dileme je bilo moč začititi tudi v podjetjih, kot sta Comtron d.o.o. in Talum d.d., ki po naši oceni sledita vsem predvidenim zakonskim določilom. Podjetje Comtron d.o.o. sklepa številne najemne pogodbe programske opreme TRONoffice. Za svoje delo pa bo podjetje potrebovalo dostop do podatkov drugega podjetja. Iz delovanja podjetja in pogodb je moč sklepati, da je podjetje Comtron d.o.o. obdelovalec podatkov.

Podjetje Comtron d.o.o. je v vlogi obdelovalca podatkov v imenu najemjojemalca. Ker bosta pogodbeni stranki imeli dostop do osebnih podatkov, morata ustrezno urediti medsebojna pogodbeno razmerja v pravnem aktu. Pogodbeni stranki morata pri sklepanju pogodbe zadostiti pogojem, ki jih je postavila Splošna uredba.

Obdelovalec je v Splošni uredbi definiran kot fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca (Evropski parlament, 2016).

Novost, ki jo je prinesla Splošna uredba, je uvedba odškodninske odgovornosti obdelovalca, ki je zapisana v 82. členu. Obdelovalec je odgovoren za škodo, ki jo je povzročil z obdelavo, kadar ne izpolnjuje obveznosti iz Splošne uredbe, ki so posebej naslovljene na obdelovalca, ali kadar je prekorščil zakonita navodila upravljavca ali ravnal v nasprotju z njimi.

Prvi odstavek 28. člena Splošne uredbe nadalje določa, da upravljavec sodeluje zgolj z obdelovalci, ki zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov na tak način, da obdelava izpolnjuje zahteve iz te uredbe in zagotavlja varstvo pravic posameznika, na katerega se nanašajo osebni podatki. V tretjem odstavku pa sta natančneje določeni obveznost sklenitve ter vsebina pogodbe med upravljavcem in obdelovalcem, ki natančneje določa obveznosti obdelovalca v razmerju do upravljavca (Pirc Musar idr., 2020).

Stranki sta zavezani upoštevati določila Splošne uredbe, saj je ta v skladu s pravom EU neposredno uporabna. To pomeni, da četudi Slovenija novega zakona o varstvu osebnih podatkov (ZVOP-2) še nima, to ni razlog za nespoštovanje uredbe, ki to ureja. Ker bosta torej pogodbenika upravljala z osebnimi podatki, morata ustrezno urediti medsebojno pogodbeno razmerje (Primec, 2019).

Splošna uredba postavlja enotna pravila za varstvo osebnih podatkov v EU, nekatera vsebinska in postopkovna vprašanja pa lahko posebej uredijo države članice. Navedeno bo urejal ZVOP-2 (Informacijski pooblaščenec, b. d.).

Kot povedano, je Splošna uredba veljavna, zavezujoča in obvezna za vsa slovenska podjetja (pa tudi za druge organizacije). Večina določb obstoječega zakona (ZVOP-1) pa je z uveljavitvijo Splošne uredbe po neobvezujoči oceni Ministrstva za pravosodje prenehala veljati. Digitalizacija skorajda vseh vidikov naših življenj in uporaba interneta v zasebnem in poslovnem okolju sta izredno razširili obseg zbiranja podatkov in pospešili pretok informacij o posameznikih. Varstvo posameznikov se s Splošno uredbo razširja tudi na tuja podjetja, ki imajo sedež izven EU, kljub temu pa poslujejo v EU in ponujajo svoje storitve evropskim državljanom oziroma obdelujejo njihove osebne podatke (Jamšek, 2018).

Ker podjetje Talum d.d. in Comtron d.o.o. delujeta tudi na trgu izven EU, se nam je zdelo vredno te primere izpostaviti.

5 Trajnostni razvoj v podjetjih

Cilji trajnostnega razvoja do leta 2030, ki si jih je zadala EU, bodo imeli ključen vpliv na razvoj podjetij. Ključna poudarka agende za trajnostni razvoj sta zeleni in digitalni prehod, ki bosta države in podjetja pripravila na krepitev odpornosti v svetu (Evropska komisija, 2022). Podjetje Talum d.d., ki smo ga proučevali v tej luči, vsekakor izpolnjuje obe začrtani agendi EU.

5.1 Zeleno podjetje

Eno izmed osnovnih vodil podjetja je skrb do okolja, varnosti in rabe energije v najširšem pomenu besede. Talum d.d. je zavezan k izpolnjevanju zakonskih in drugih zahtev (Čuš idr., 2022).

Talum d.d. se po svoji velikosti uvršča med podjetja, ki spadajo na področje uporabe določb Energetskega zakona (EZ-1). Podjetje ima tudi dva statusa – status odprtega distributerja električne energije in status zaprtega distributerja zemeljskega plina. Podjetje se torej zaveda svoje pomembne vloge na področju reševanja okoljskih in podnebnih izzivov. Tako med drugim trguje s CO₂-kuponi (S. Horvat, osebna komunikacija, 20. 4. 2022).

V podjetju so v zadnjem desetletju intenzivirali preoblikovanje svoje proizvodnje v smeri ogljično nevtralnih izdelkov iz aluminija z visoko dodano vrednostjo in v smeri reciklaže različnih vrst odpadnega aluminija, iz katerega potem delajo nove izdelke (Čuš idr., 2022).

Z investicijami v razvoj, modernizacijo in nadgradnjo obstoječih BAT-tehnologij, vpeljavo novih tehnologij in varstva okolja je podjetje Talum d.d. že izpolnilo cilj »Pripravljeni na 55« do 2030, saj je skupni ogljični odtis iz neposrednih izpustov CO₂ zmanjšalo za 79 odstotkov (Čuš idr., 2022).

Omeniti je treba, da je trgovanje s pravicami do izpusta toplogrednih plinov pomemben temelj strategije Evropske unije in njenih držav članic pri zmanjševanju izpustov toplogrednih plinov. Trgovanje za Talum d.d. predstavlja velik izziv, saj podjetje pričakuje, da bo dolgoročno v veliki meri znižalo stroške zmanjševanja izpustov (Sektor za podnebne spremembe in biotehnologijo, b. d.).

5.2 Digitalno podjetje

Digitalizacijo na pravnem področju v podjetju Talum d.d. je pravilneje imenovati informatizacija. Večinoma gre za uvedbo informacijskih rešitev v organizacijo, predvsem z namenom optimiziranja njenega notranjega poslovanja (Štempihar, b. d.).

Na področju delovnih razmerij je v podjetju vzpostavljena digitalna kadrovska mapa. Izziv za podjetje je, kako zagotoviti, da bo pogodba o zaposlitvi sklenjena v elektronski obliki. Cilj je vsekakor brezpapirno poslovanje, da bodo zaposleni dostopali do svojih dokumentov, ki jih imajo v delovnem razmerju v kadrovskih mapah (S. Horvat, osebna komunikacija, 20. 4. 2022).

Delodajalec s personalno mapo zaposlenega vodi vse pomembne podatke za izpolnjevanje pravic in obveznosti iz delovnega razmerja. Kako točno mora delodajalec voditi seznam evidenc, je določeno z Zakonom o delovnih razmerjih (ZDR-1) in Zakonom o evidencah na področju dela in socialne varnosti (ZEPDSV). Nadalje je v ZDR-1 v 48. členu določen način varovanja delavčevih osebnih podatkov, zato so njegovi podatki varni in jih delodajalec ne sme zlorabiti. Prav tako delodajalec zaradi varovanja osebnih podatkov ne sme shranjevati fotokopij osebnih dokumentov. Po navadi personalna mapa zaposlenega vsebuje predlog pogodbe o

zaposlitvi in izjavo o prevzemu predloga pogodbe, podpisano pogodbo o zaposlitvi in izjavo o prevzemu enega izvoda pogodbe o zaposlitvi, aneks ter obrazec Evidenčni list zaposlenega. Poudariti pa je treba, da vsebina mape ni predpisana in so to le okvirne komponente (EVem, 2016).

Poleg tega pa je treba razumeti, da je v podjetju Talum d.d. zaposleno veliko število starejših delavcev v proizvodnji. Pomembno je, da podjetje delavce izobražuje v tej smeri, jim približa način uporabe in na sploh pomaga pri digitalni pismenosti. Tako bodo zaposleni lahko dostopali do svojih dokumentov, ki jih imajo v kadrovske mapi (S. Horvat, osebna komunikacija, 20. 4. 2022).

Iz pogovorov s predstavniki podjetja je bilo moč zaznati, da je bil velik napredek opravljen predvsem v zadnjem času ob nastopu pandemije covid-19. Podjetje je v tem času še pospešilo informatizacijo svojih zaposlenih (S. Horvat, osebna komunikacija, 20. 4. 2022).

6 Zasebnost na delovnem mestu

Zaradi procesa digitalizacije in razvoja informacijske tehnologije je vprašanje zasebnosti na delovnem mestu vse bolj kompleksno, izvajanje nadzora nad delom zaposlenih pa dosti lažje, kot je bilo pred leti (Brajnik, 2019). Predvsem razvoj informacijsko-komunikacijske tehnologije je občutno spremenil tudi delovnoppravna razmerja.

Pri obdelavi osebnih podatkov v razmerju delavec – delodajalec je treba upoštevati in razumeti tako interese delodajalca kot tudi interese delavca. Ugotavljanje delovne uspešnosti, čim bolj racionalna izraba delovnega časa in delovnih sredstev, učinkovitost in varnost delovnega procesa ter nadzor nad njim in preprečevanje morebitnih zlorab so argumenti, ki delodajalce ženejo k nadzoru zaposlenih. Kljub temu pa bi nad interesi močnejšega delodajalca v določenih okoliščinah morala prevladati pravica šibkejšega delavca do zasebnosti, do katere je (seveda v razumnih mejah) upravičen tudi na delovnem mestu. Delavca je treba obravnavati kot posameznika, ki ima poleg obveznosti iz delovnega razmerja tudi pravice osebne narave (Varstvo osebnih podatkov, b. d.).

Ključno je, da se delodajalec zaveda, da lahko prekomeren nadzor in posegi v delavčev zasebno sfero zaposlenim povzročijo dodaten stres. Takšni delavci bodo na delo prihajali manj zadovoljni ter posledično tudi manj produktivni in motivirani. To so tudi razlogi, da se delavcem poslabša zdravstveno stanje, koristijo več bolniške odsotnosti ali menjajo zaposlitev in se zaposlijo pri delodajalcu, kjer imajo večji občutek zasebnosti. (Brajnik, 2019).

To je le nekaj razlogov, ki so delodajalcem lahko v opomin pri tem, kako bodo svojim delavcem pojasnili, da digitalizacija in informatizacija delovnega procesa ne predstavljata vdora v njihovo zasebnost. Po drugi strani pa se morajo delodajalci sami ustrezno omejiti in sprejeti ustrezne pravne podlage, ki morajo biti skladne s slovensko in evropsko zakonodajo.

Četudi so delavci v razmerju z delodajalcem šibkejša stranka, to ne pomeni, da morajo dopustiti kakršne koli posege v svojo zasebnost. ZDR-1 določa, da morajo delodajalci zaposlenim zagotavljati varne delovne razmere, spoštovati delavčev osebno ter upoštevati in ščititi delavčev zasebnost (45. in 46. člen ZDR-1). Vse to spada pod delodajalčeve obveznosti.

Delodajalec ima pravice, ki izvirajo iz njegove lastnine nad delovnimi sredstvi, delavec pa ima nedvoumno tudi na delovnem mestu pravico do zasebnosti. Pristojnosti delodajalca do nadzora na delovnem mestu in pravic delavca do zasebnosti na delovnem mestu v Sloveniji izrecno (še) ne ureja noben zakon. Uporaba biometrijskih ukrepov in videonadzor na delovnem mestu sta sicer trenutno urejena v ZVOP-1, medtem ko še nimamo zakona, ki bi podrobneje urejal uporabo interneta, elektronske pošte, telefonov, GPS-sledilnih naprav ipd. na delovnem mestu (Varstvo osebnih podatkov, b. d.).

Ukrepe, s katerimi bi delodajalec omejeval pravico do zasebnosti, je dopustno vpeljati v delovni proces le pod posebej določenimi pogoji, ki so v nekaterih primerih izrecno opredeljeni v zakonu ali drugih predpisih. Vsem mehanizmom nadzora zaposlenih je skupno to, da je treba v prvi vrsti oceniti, ali je določena obdelava osebnih podatkov skladna z načelom sorazmernosti, ter nato ugotoviti, pod katerimi pogoji je tudi zakonita (Brajnik, 2019).

Pomembno vodilo razmerja med strankama v delovnem razmerju je, da je obdelava osebnih podatkov dopustna le, če imajo delodajalci zanje ustrezno pravno podlago. Splošna uredba vsebuje številne varovalke, preko katerih se nadzoruje delodajalca s ciljem preprečitve izvajanja nedopustnega nadzora. Pri izvajanju sistematičnega nadzora je delodajalec precej omejen. Vsak tak nadzor bi moral utemeljiti z eno izmed pravnih podlag po Splošni uredbi (Polajžar, 2020). V okviru delovnega razmerja za obdelovanje osebnih podatkov je na tem mestu smotno omeniti splošne pravne podlage za obdelavo osebnih podatkov, kot so določene v 6. členu Splošne uredbe o varstvu podatkov.

Hkrati je vredno omeniti tudi določbe ZDR-1. Zaradi neenakega položaja delodajalca do delavca slednjega varuje ZDR-1, ki v 48. členu določa, da delodajalec ne sme zbirati katerih koli osebnih podatkov, ampak le tiste, ki jih potrebuje za dosego v zakonu določenega namena (Varstvo osebnih podatkov, b. d.).

7 Sklep

Podjetji Talum d.d. in Comtron d.o.o. se zavedata sodobnih izzivov, ki jih prinaša proces digitalizacije. To je predvsem opazno z vpeljevanjem naprednih tehnologij in orodij, ki vodijo do postopnega preoblikovanja v pametno tovarno z visoko stopnjo avtomatizacije, robotizacije in digitalizacije procesov.

Podjetje Comtron d.o.o. je poleg inovativnih tehnologij, ki jih razvija, ustrezno naslovilo vsa pravna razmerja v pogodbah, ki se tičejo varstva zasebnosti njegovih zaposlenih in strank. Hkrati smo skozi sodelovanje odprli številne aktualne razvojne preizkušnje digitalizacije in njihovo pravno regulacijo, ki so postavljene pred EU. Iz pogovora z vodjo pravne službe in proučitve podjetja Talum d.d. je bilo mogoče dobiti občutek, da se podjetje zaveda posameznih pravnih dilem, ki jih je prinesel proces digitalizacije. Podjetje se zaveda, da je vpeljava novih tehnologij in digitalnih rešitev neizbežna. Obenem pa krepi dober odnos z zaposlenimi, ki jih je prav tako treba soočiti z vpeljavo novih digitalnih izzivov. Sočasno podjetje odlikuje tudi odlično poznavanje ne le slovenske, ampak tudi evropske zakonodaje glede zasebnosti in varstva osebnih podatkov posameznika. Ocenjujemo, da obe podjetji sledita visokim standardom spoštovanja človekovih pravic ter temeljnim vrednotam EU.

Literatura

- Andrejek, N. (2019). Obveznosti ponudnika zaradi varnosti podatkov in varstva osebnih podatkov pri računalništvu v oblaku [Magistrsko delo, Univerza v Ljubljani, Pravna fakulteta]. Repozitorij UL. <https://repozitorij.uni-lj.si/Dokument.php?id=120656&lang=slv>
- Brajnik, M. (5. 8. 2019). *Nadzor zaposlenih na delovnem mestu*. IUS-INFO. <https://www.iusinfo.si/medijsko-sredisce/v-srediscu/247067#3>
- Brkan, M. (9. 3. 2020). *Digitalizacija v Evropski uniji: pravne in dejanske dileme*. IUS-INFO. <https://www.iusinfo.si/medijsko-sredisce/kolumne/258855>
- Čuš, Z., Homšak, M., Lipovac, K., Trafela, I., Gajšt, J., Vodušek Vtič, D., Vodušek Fras, N., in Kores, S. (2022). *Okolje, energija ter varnost in zdravje pri delu v Skupini Talum*. Talum. https://www.talum.si/pdf/Okolje_%20energija_%20ter_%20varnost_%20in_%20zdravje_%20pri_%20delu_%20v_%20Skupini_%20Talum-maj_%202022.pdf
- EVem. (3. 8. 2016). *Personalna mapa zaposlenega*. <http://www.evem.si/personalna-mapa-zaposlenega/>
- Evropska komisija (2022). Celostni pristop EU k trajnostnemu razvoju. https://ec.europa.eu/info/strategy/international-strategies/sustainable-development-goals/eu-holistic-approach-sustainable-development_sl
- Evropski parlament. (2016). 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)
- Evropski parlament. (2022). Kibernetska varnost: najnevarnejše in rastoče grožnje (infografika). <https://www.europarl.europa.eu/news/sl/headlines/society/20220120STO21428/kibernetnska-varnost-najnevarnejse-in-rastocje-groznje-infografika>
- Informacijski pooblaščenec. (b. d.). Najpogostejša vprašanja in odgovori. <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnihpodatkov/najpogostejsa-vprasanja-in-odgovori>
- Jamšek, B. (20. 11. 2018). GDPR: Uredba o varstvu podatkov. Mladi podjetnik. <https://mladipodjetnik.si/novice-in-dogodki/novice/gdpr-uredba-o-varstvu-podatkov>
- Lobo, N.-M. (3. 12. 2020). Responsibilities of a Controller, Processor & Data Protection Officer. WSI. <https://www.wsiworld.com/blog/responsibilities-of-a-controller-processor-and-data-protection-officer-according-to-gdpr>
- Pirc Musar, N., Lemut Strle, R., Remic, M., Drev, M., Kraigher Mišič, K., Poljšak, A., Kraigher Mišič, T., Rostohar, I., Medved, K., Voga, M., Lubarda, M., Tomaduz, U. in Emeršič Polič, K. (2020). Komentar Splošne uredbe o varstvu podatkov. Uradni list RS
- Polajžar, A. (2020). *Meje dopustnega nadzora delavcev z in pri uporabi sredstev informacijsko komunikacijske tehnologije na delovnem mestu: izbrani vidiki* [Magistrsko delo]. Univerza v Mariboru, Pravna fakulteta.
- Posel se seli v zasebni oblak Microsoft Azure na Pošti Slovenije. (24. 6. 2020). Finance.si. <https://www.finance.si/8963289/Posel-se-seli-v-zasebni-oblak-Microsoft-Azure-na-Posti-Slovenije>
- Primec, A. (2019). Varstvo osebnih podatkov v podjetju: priročnik za mala in srednja podjetja. Univerzitetna založba Univerze v Mariboru.
- Sektor za podnebne spremembe in biotehnologijo. (b. d.). *Trgovanje s pravicami do emisije*. <https://www.gov.si teme/trgovanje-s-pravicami-do-emisije/>
- Štampihar, A. (b. d.). *Digitalnost > informatizacija*. Mikrocop. <https://www.mikrocop.si/blog/digitalnost-informatizacija>
- Varstvo osebnih podatkov v delovnih razmerjih: Smernice informacijskega pooblaščenca*. (b. d.). Informacijski pooblaščenec. https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_-_Varstvo_OP_v_delovnih_razmerjih_verzija_1.1_končna.pdf
- Vključevanje delavcev in upravljanje - ozaveščanje, preizkus, spremljanje: Regionalni pregled in prihodnji trendi*. (2017). Združenje delodajalcev Slovenije
- Zakon o varstvu osebnih podatkov (ZVOP-1). (2004). Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20. <http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906>

