



REPUBLIKA SLOVENIJA

INFORMACIJSKI POOBLAŠČENEC

Dunajska cesta 22, 1000 Ljubljana
T: 01 230 9730
F: 01 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Številka: 0613-66/2018/11

Datum: 4. 10. 2022

Informacijski pooblaščenec (v nadaljevanju IP) izdaja po državnem nadzorniku za varstvo osebnih podatkov Blažu Pavšiču na podlagi 2. in 8. člena Zakona o informacijskem pooblaščenecu (Uradni list RS, št. 113/05 in 51/07 – ZustS-A, v nadaljevanju: ZInfP), 37. in 54. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07-UPB1 in 177/20, v nadaljevanju: ZVOP-1), petega odstavka 29. in prvega odstavka 32. člena Zakona o inšpekcijskem nadzoru (Uradni list RS, št. 43/07 – UPB1 in 40/14, v nadaljevanju: ZIN) ter členov 57(1) in 58(2) Uredbe (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 razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov, v nadaljevanju: Splošna uredba), v postopku inšpekcijskega nadzora pri zavezancu _____ (v nadaljevanju: zavezanec), po uradni dolžnosti naslednjo

ODLOČBO

1. Zavezanec mora **v roku 10 dni od vročitve** te odločbe prenehati s pridobivanjem in shranjevanjem lokacijskih osebnih podatkov zaposlenih, ki jih pri izvajanju sistematičnega, avtomatiziranega in kontinuiranega GPS sledenja službenih vozil pridobiva in zbira na način, da s pomočjo GPS sledilnih naprav, nameščenih v službenih vozilih, sledi gibanju teh vozil in na ta način pridobljene lokacijske podatke tudi shranjuje.
2. Zavezanec mora **v roku 10 dni od vročitve** te odločbe prenehati z izvajanjem videonadzora delovnih prostorov – proizvodnje, ki jih izvaja s petimi videokamerami (kamere št. 3, 4, 7, 8 in 9) in te kamere iz teh prostorov odstraniti.
3. Zavezanec mora o izvršenih ukrepih iz 1. in 2. točke izreka te odločbe **v roku 5 dni po izvršitvi** pisno obvestiti IP in predložiti dokaze o tem.
4. V tem postopku posebni stroški niso nastali.

Obrazložitev:

I. Ugotovitve IP ter pojasnila in stališča zavezanca

IP je postopek inšpekcijskega nadzora pri zavezancu začel na podlagi prijav, v katerih so prijavitelji navajali sume nepravilnosti pri obdelavi osebnih podatkov zaposlenih, ki jo izvaja zavezanec pri in v zvezi z uporabo sistema GPS sledenja njegovih službenih vozil in nepravilnosti pri izvajanju videonadzora s strani zavezanca.

Zavezanec je v svojem prvem odgovoru na poziv IP navedel, da se je za sledenje svojih službenih tovornih vozil odločil v oktobru 2009 in da ga od takrat izvaja s pomočjo opreme, ki jo najema pri zunanjem ponudniku opreme. Vsa vozila, v katera so nameščene GPS naprave (skupaj sedem) naj bi bila v lasti zavezanca in naj jih zaposleni izven delovnega časa, za zasebne namene, ne bi uporabljali. Uporabljali naj bi jih izključno za potrebe dela na terenu tj. za potrebe prevoza in montaže opreme pri naročnikih zavezanca. Za izvedbo GPS sledenja naj bi se zavezanec odločil, ker je želel zavarovati vozila, drago opremo in dokumente, ki se nahajajo v vozilih (vrednost opreme in vozila naj bi lahko presegala znesek 100.000 eurov) tj. zaradi preprečevanja kraje vozil, opreme in dokumentov, ki se nahajajo v vozilu in izsleditev tega v primeru kraje. Opisane namena naj zavezanec na drugačen način, ne bi mogel doseči. Zavezanec je navedel, da GPS sledenje uporablja na podlagi seznanitve zaposlenih, ki vozila uporabljajo in dodal, da na nameščeno opremo zaposlene izrecno opozarjajo tudi nalepke, ki se nahajajo v vozilih. V pripravi naj bi bil tudi pravilnik, ki naj bi pri zavezancu dodatno uredil to področje. GPS sledenje naj bi zavezanec uporabljal tako, da z njim ne zbira nobenih osebnih podatkov, saj naj se sledenje ne bi vršilo nad zaposlenimi, ampak izključno nad vozili. V uporabljeni programski opremi naj bi bila razvidna zgolj registrska številka vozila in njegova trenutna lokacija ter prevožena pot, ne pa tudi podatek o trenutnem vozniku oz. uporabniku vozila oz. osebah, ki se z njim vozijo. Dobavitelj opreme naj bi ponujal tudi druge funkcije vgrajene opreme za sledenje (vodenje potnih nalogov, analiza podatkov o voznem parku, ipd.), vendar naj se zavezanec za njihovo uporabo ne bi odločil. Zavezanec je v svojem odgovoru navedel tudi, da zbranih podatkov (o trenutni lokaciji oz. opravljeni poti posameznega vozila) ne obdelujejo in da se podatki po določenem času avtomatsko izbrišejo. Zbranih podatkov naj zavezanec ne bi uporabljal za nadzor zaposlenih, niti naj to na podlagi avtomatsko zbranih podatkov (lokacija oz. pot v povezavi z registrsko številko vozila), ob odsotnosti povezave navedenih podatkov s posamezno osebo, ne bi bilo mogoče. Zavezanec je navedel še, da opremo za GPS sledenje najema pri zunanjem dobavitelju opreme, družbi _____, da pa samo sledenje izvaja sam oz. njegov direktor, ki naj bi imel tudi edini dostop do aplikacije in vpogled vanjo ter v njej zbrane podatke. Do aplikacije in podatkov naj bi dostopal s pomočjo svojega uporabniškega imena in gesla. Poleg navedenih pojasnil je zavezanec IP posredoval tudi kopijo pogodbe z družbo _____, fotografijo opozorilne nalepke v enem od vozil, seznam vozil, v katerih ima nameščene sledilne naprave, dokument s podatki vstopov v sistem in kopijo poročila postankov vozila za določeno obdobje.

V svojem drugem odgovoru na poziv IP je zavezanec dodatno navedel, da se v njegovih službenih tovornih vozilih lahko nahaja draga oprema potrebna za delo, načrti last zavezanca, izdelki, polizdelki, material potreben za delo itd. Vrednost opreme v vozilu naj ne bi bila vedno enaka, zavezanec pa naj bi jo ocenjeval glede na vrednost posameznega aparata, materiala, izdelka ali polizdelka, načrtov in pa vrednosti samega tovornega vozila. Zavezanec je IP poslal račun za enega od aparatov, potrebnih za delo na terenu in ob tem navedel, da ta oprema ni vedno v tovornem vozilu in da se lahko transportira samo material potreben za delo na terenu, lahko pa se zgodi, da se v vozilu nahajata dva taka aparata. Poleg tega naj bi bili tu še načrti zavezanca, katerih vrednost naj bi bilo težje opredeliti. Zavezanec je navedel, da ker se tovorna vozila ne uporabljajo za zasebne namene oz. izven delovnega časa vgradnja privat/službenega stikala naj ne bi bila potrebna. Poleg tega naj bi bil to neavtomatiziran ter tako nezanesljiv proces in bi lahko prihajalo do človeških napak (zaposleni naj bi lahko pozabil vključiti/izključiti napravo), tak način pa naj bi pomenil tudi dodano obveznost in obremenitev za zaposlene. Zaposlene naj bi zavezanec z uvedbo sistema GPS sledenja tovornih vozil obvestil ob sklenitvi pogodbe z družbo _____ in sicer ustno in z obvestilom na oglasni deski. Vse novo zaposlene naj bi s tem seznanili ustno ob začetku zaposlitve. Zavezanec je v svojem odgovoru navajal, da s pomočjo aplikacije za GPS ne morejo ugotoviti, kdo je uporabnik vozila in da podatki o registrski številki vozila, trenutni lokaciji ter prevoženih kilometrih niso podatki, iz katerih bi bilo razvidno, kdo je uporabnik vozila. Po navedbah zavezanca pri njem uporabljajo potne naloge, ki jih

izpolnjujejo ročno in da pri tem uporabljajo standardni obrazec, ki je sestavljen iz dveh delov. Prvi del obrazca naj bi izpolnil vodja posameznega oddelka, ki zaposlenega napoti na službeno pot oz. delo na terenu, drugi del pa naj bi izpolnil zaposleni sam. Zavezanec je IP poslal tudi primer obrazca, iz katerega je razvidno, katere podatke vsebuje posamezen potni nalog. V službenih tovornih vozilih naj bi se poleg tega nahajal tudi potni nalog za vozilo, ki naj bi ga zavezanec dobival v pregled enkrat mesečno. IP je zavezanec posredoval tudi premer tega obrazca. V zvezi z vpogledi v osebne podatke, ki so bili pri zavezancu zbrani z izvajanjem GPS sledenja je zavezanec navedel, da so bili vsi vpogledi informativne narave kot npr. vpogled zaradi kontrole delovanja sistema. Zavezanec je navedel tudi, da GPS sistema ni uvedel z namenom nadzora nad delom zaposlenih in da nobeden od preteklih vpogledov ni bil namenjen izvajanju takega nadzora.

V svojem odgovoru na dodaten poziv IP je zavezanec navedel, da imajo GPS tehnologijo vgrajeno v osem službenih vozil, ki se uporabljajo za potrebe dela na terenu v službenem času tj. za potrebe prevoza materiala, opreme in montaže opreme pri naročnikih, sestanke z naročniki, itd. Ta vozila naj bi uporabljali predvsem delavci proizvodnje, ki odhajajo na teren ter projektanti. Zavezanec naj bi imel dve službeni vozili, ki nimata vgrajene GPS tehnologije in sicer zato, ker naj bi se uporabljali tudi izven delovnega časa oziroma za zasebne namene. Zavezanec je navedel, da naj bi do obdelave osebnih podatkov z uporabo GPS tehnologije lahko prišlo zgolj izjemoma, saj naj uvedena tehnologija funkcionalnosti beleženja potnih nalogov ter osebnih podatkov zaposlenih ne bi imela. Do obdelave osebnih podatkov naj bi prišlo v izjemnih primerih in sicer na podlagi točke f) prvega odstavka člena 6 Splošne uredbe v povezavi z 48. členom ZDR-1, pri čemer naj bi bili zakoniti interesi za katere si prizadeva zavezanec zlasti varnost in zaščita opreme in dokumentov, ki se nahajajo v vozilih, preprečevanje protipravnega odvzema vozil, varnost zaposlenih, določitev lokacije v primeru prometne nesreče, uveljavljanje in obramba morebitnih pravnih zahtevkov, itd. GPS tehnologija naj bi bila uvedena po tem, ko je prišlo do kraje na delovišču, vloma in poškodovanja lastnine zavezanca, slednji pa naj bi se zanjo odločil s ciljem varovanja premoženja družbe in varnosti zaposlenih. Njegov namen naj ne bi bila obdelava osebnih podatkov zaposlenih ali sledenje posameznikom, ampak naj bi odločitvi botrovale posebne okoliščine službenih poti (premoženje in dokumentacija večje vrednosti v vozilu, službene vožnje na bolj odročne lokacije, ipd.). Od uvedbe GPS sledenja naj do kaznivih dejanj in škodnih dogodkov ne bi prišlo, zato naj zavezanec do osebnih podatkov, ki jih je zbral z GPS sledenjem ne bi dostopal ali jih izpisoval. Zavezanec je navajal, da GPS sledenje, kot ga izvaja, ne obsega obdelave osebnih podatkov zaposlenih in da bi take obdelave lahko prišlo v primeru povezave z GPS sistemom zbranih podatkov s potnim nalogom za službeno pot, kar naj bi imel evidentirano v Evidenci uporabe GPS tehnologije. Obdelava osebnih podatkov naj bi se tako izvedla izključno v posebej utemeljenih primerih (kazniva dejanja, varovanje ljudi in premoženja, pomoč pri prometni nesreči, škodni dogodki, ipd.) oziroma takrat, ko bi bila uporaba takega podatka nujna in sorazmerna za zagotavljanje zakonitega interesa zavezanca, v nasprotnem primeru pa naj se povezava posameznika s podatki iz sistema GPS ne bi vršila. Zavezanec je navedel, da so potni nalogi del posebne evidence ter se hranijo v zavarovani omari, do GPS aplikacije pa dostopa z računalniškim programom in da neposredne povezave med evidencama ni. Glede na navedeno zavezanec šteje, da gre za sorazmeren obseg obdelave osebnih podatkov, ki naj, zaradi navedene omejene obdelave, ne bi bil v škodo zaposlenih, ki uporabljajo službena vozila. Zavezanec je navedel, da so zaposlene z uvedbo GPS tehnologije seznanili ob sklenitvi pogodbe z družbo _____ - in sicer ustno ter pisno (z izjavo) ter s pisnim obvestilom na oglasni deski, ki naj bi bilo pri zavezancu običajno sredstvo za obveščanje zaposlenih. Vse novo zaposlene naj bi z uporabo GPS tehnologije seznanili pred in ob začetku zaposlitve. Zavezanec naj bi obvestilo po uveljavitvi Splošne uredbe nekoliko dopolnil in naj bi bilo vsem zaposlenim na voljo na oglasni deski. Zaposlene naj bi torej s tehnologijo seznanjali redno, ustno in pisno, zaposleni pa naj bi podpisali izjavo o seznanitvi. V letu 2018 naj bi zavezanec področje dodatno uredil s sprejetjem pravilnika. V primeru vprašanj zaposlenih v zvezi s

podatki, ki se ob uporabi GPS sledenja obdelujejo naj bi jim bil zavezanec vedno na voljo, zaposlene pa naj bi na nameščeno opremo izrecno opozarjale nalepke, ki se nahajajo v oziroma na vozilih. Da zavezanec z GPS tehnologijo neposredno ne obdeluje osebnih podatkov zaposlenih in da to ni njegov namen naj bi izhajalo iz revizijske sledi izpisa podatkov, ki se spremljajo in pojasnila družbe _____, ki jih je zavezanec posredoval IP. Podatki, ki jih zavezanec pridobi s to tehnologijo naj bi se nanašali na vozila in ne na posameznike, ki naj bi bili sicer določljivi, a ob vgrajenem varnostnem mehanizmu, ki neposredne povezave ne omogoča, zaščiteni in uporabljeni izključno takrat, ko bi bilo to potrebno zaradi zakonitih interesov zavezanca ter za zaščito življenjskih interesov posameznika, ki vozilo vozi in se mu npr. pripeti nesreča, tatvina, rop, ipd.

Aplikacija _____ naj bi spremljala podatke o lokaciji službenega vozila v določenem trenutku (datum/ura), opravljeni poti službenega vozila (kilometri, pozicija) in registrski številki vozila. Navedene podatke naj bi vodila in hranila družba _____, kot izvajalec, ki naj bi sicer ponujala tudi storitev povezave z osebnimi podatki zaposlenih, vodenje potnih nalogov, podatkov o voznem parku, ipd, a naj se zavezanec za te funkcionalnosti ne bi odločil, ker jih ne potrebuje in naj bi štel, da namene za uvedbo GPS sledenja izpolnjuje z obdelavo podatkov v opisanem, sorazmernem obsegu. Podatki o zaposlenih naj se tako v aplikaciji ne bi obdelovali, družba _____ pa naj do njih ne bi mogla dostopati in naj tudi sicer ne bi razpolagala z nikakršnimi podatki o zaposlenih pri zavezancu, niti naj se ti ne bi nahajali v aplikaciji, kjer naj bi bilo spremljanje podatkov v celoti anonimno. Do podatkov zaposlenih naj bi dostopale izključno pooblaščen osebe tj. direktor zavezanca. Z uporabo aplikacije naj bi zavezanec dostopal do podatka, kje se vozilo nahaja in kdaj, vstop v aplikacijo pa naj bi bil mogoč z osebnim uporabniškim imenom in geslom. Zavezanec je navedel, da v podatke, ki jih hrani aplikacija do podaje odgovora še niso vpogledovali oziroma so družbo _____ za izpis podatkov zaprosili dvakrat in sicer v obeh primerih za potrebe priprave odgovora na poziv IP. Zavezanec je IP posredoval tudi izpis, kakršen naj bi se generiral ob zahtevi za vpogled podatkov in pojasnilo družbe _____. Slednja družba naj bi lahko z zbranimi podatki pripravila poročilo (npr. poročilo o voznjah za posamezno vozilo), vendar naj se zavezanec te možnosti ne bi posluževal, saj naj analiz ne bi opravljal. Občasno naj bi opravil pregled oziroma vpogled v sistem informativne narave, s katerim naj bi se zgolj preverilo delovanje GPS sistema. V obdobju od 1. 1. 2021 naj bi bilo na ta način v aplikacijo vpogledano dvakrat. Podatki, ki jih zavezanec pridobi z GPS sledenjem naj bi se v programu hranili eno leto, po tem času pa naj bi se podatki trajno izbrisali. Zavezanec je v zvezi z GPS sledenjem IP posredoval naslednje dokumente (dokumenti kot jih je poimenoval zavezanec): Seznam vozil z GPS tehnologijo, Pravilnik o izvajanju GPS sledenja, Obvestilo zaposlenim iz člena 14 Splošne uredbe (objavljeno na oglasni deski zavezanca), Izjava zaposlenih (vzorec), Evidenca osebnih podatkov, ki nastaja z uporabo GPS sledenja, Evidenca uporabe službenih vozil in potnih nalogov, Revizijska sled vpogledov v podatke aplikacije GPS sledenja z izpisom vpogledanih podatkov, elektronsko sporočilo družbe _____ in elektronsko sporočilo družbe _____.

V zvezi z izvajanjem videonadzora je zavezanec navedel, da imajo devet videokamer, ki so nameščene na vhodu/izhodu stavbe podjetja, na dvorišču – na mestu, kjer se hrani tudi material in v proizvodnji, kjer se nahajajo naprave in oprema večje vrednosti in naprave, ki so lahko izjemno nevarne za zdravje in življenje zaposlenih. V letu 2017 naj bi se vodstvo zavezanca, iz razlogov varovanja ljudi in premoženja odločilo za postavitev kamer in hkrati tudi senzorjev za alarmiranje požara in vloma, v skladu s tem pa naj bi bil izdelan in postavljen sistem požarnega javljanja in videonadzora, z namenom aktivne požarne varnosti in vloma, zaščite premoženja in lastnine delodajalca, zaščite delavcev in obiskovalcev, zagotavljanja nadzora vstopa in izstopa v/iz službenih prostorov podjetja ter tudi zato, ker naj bi zaradi narave dela obstajala možnost ogrožanja zaposlenih. Z videonadzorom naj se ne bi izvajalo nadzora nad delom zaposlenih, postavljeni sistem naj niti ne bi omogočal določljivega pregledovanja videoposnetkov in nadzora nad delom, kar naj bi

bilo razvidno iz zaslonskih slik, ki jih je IP predložil zavezanec. O izvajanju videonadzora naj bi bili zaposleni obveščeni ustno in pisno (z izjavo) ter z objavo obvestila na oglasni deski, ki naj bi bilo pri zavezancu običajno sredstvo za obveščanje zaposlenih. Vse novo zaposlene naj bi z lokacijami izvajanja videonadzora seznanili pred in ob začetku zaposlitve, vsem zaposlenim pa naj bi bilo obvestilo dostopno na oglasni deski. Snemalna naprava naj bi se nahajala v za to namenjenem prostoru zavezanca, do katerega naj bi dostopal zaposleni na delovnem mestu informatika. Prostor pa naj bi bil varovan s fizičnim zaklepanjem, upravljanje naprave za snemanje pa naj bi bilo dostopno z osebnim geslom. Dostop do žive slike naj bi bil omogočen preko aplikacije na računalniku, ki naj bi prav tako zahtevala osebno geslo za dostop do računalnika in potem še posebno geslo za dostop do aplikacije. Posnetki naj bi se na snemalni napravi hranili en teden, potem pa naj bi se izbrisali, razen v primeru, da se iz posebej utemeljenega razloga zavarujejo do pravnomočnega končanja postopka, zaradi katerega so bili zavarovani. Oddaljen dostop naj bi imela omogočen direktorja podjetja in sicer za primer javljanja požarnega ali vlomnega alarma, na ta način pa naj bi lahko pravočasno zagotovila priklic gasilcev, varovanja, ipd. Dostop do snemalne naprave naj bi imela izključno pooblaščen oseba in sicer informatik, dostopanje preko aplikacije pa naj bi bilo omogočeno z uporabniškim imenom in geslom. Z dostopom preko aplikacije naj bi se v aplikaciji avtomatsko zabeležil dostop z samo registracijo v aplikacijo (uporabniško ime), kar naj bi zagotavljalo sledljivost podatkov. Informacija o vpogledih v videoposnetke (sledljivost), naj bi bila razvidna iz Evidence uporabe videonadzornega sistema, ki jo je zavezanec priložil svojemu odgovoru. Zavezanec naj bi videonadzor izvajal sam, dostop do podatkov pa naj bi bil omogočen samo posebej pooblaščenim zaposlenim in sicer direktorju in informatiku, delno pa tudi zaposlenim v nabavni službi, ki skrbijo za odpiranje vhodnih vrat dobaviteljem (nabavna služba naj bi spremljala izključno posnetke vhoda in izhoda iz poslovnih prostorov ter skrbela za odpiranje vrat dobaviteljem in strankam). Obvestila o izvajanju videonadzora naj bi se nahajala na vhodu v stavbo, na vhodu na dvorišče in na vhodu v proizvodnjo, kar naj bi bilo razvidno tudi iz fotografij, ki jih je svojem odgovoru priložil zavezanec. Poleg že navedenih dokumentov je zavezanec IP posredoval tudi zaslonske slike videokamer, Obvestilo zaposlenim o izvajanju videonadzora, objavljeno na oglasni deski, vzorec izjave zaposlenih, Sklep o uvedbi videonadzora, Pravilnik o videonadzoru in Evidenco videonadzora.

IP je zavezanca pisno seznanil s svojimi ugotovitvami v predmetnem inšpekcijskem postopku in ukrepi, ki jih bo moral glede na te ugotovitve v postopku sprejeti ter mu dal možnost, da se opredeli do vseh ugotovljenih dejstev in okoliščin v postopku. Zavezanec je v svojem odgovoru na seznanitev in poziv navedel, da pri GPS sledenju službenih vozil ne gre za kontinuirano in sistematično sledenje. Navedeno tehnologijo naj bi uvedli po tem, ko je prišlo do karaje na delovišču, vloma in poškodovanja lastnine zavezanca, torej dejanskega oškodovanja njegovega premoženja in ne zgolj zaradi verjetnosti, da bo do nevarnosti prišlo. Za obravnavano sledenje naj bi se odločili izključno zaradi varovanja premoženja zavezanca in varnosti zaposlenih in nikakor ne zato, da bi obdelovali osebne podatke zaposlenih, ali jih na kakršenkoli način sledili, kar naj bi potrjeval tudi sistem sledenje, ki naj v zvezi z delavci ne bi beležil ničesar. Sistem naj bi beležil le pot vozila, katere pa naj brez posebej utemeljene okoliščine, zaradi katere bi izvedli vpogled v evidenco zaposlenih, z delavci ne bi povezovali oz. naj to od uvedbe sledenja ne bi naredil še nikoli, saj naj do škodnih dogodkov od takrat še ne bi prišlo, zaradi česar naj do osebnih podatkov v povezavi z GPS podatki ne bi dostopali ali jih izpisovali. GPS tehnologija naj bi bila pri zavezancu v uporabi za potrebe dela na terenu v delovnem času tj. za potrebe prevoza materiala, opreme in montaže opreme pri naročnikih, sestankih z naročniki itd., pri čemer naj ne bi držala ugotovitev IP, da se lahko enak namen zagotavlja brez uporabe te tehnologije. Šlo naj bi namreč za posebne okoliščine službenih poti (premoženje večje vrednosti, službene vožnje na bolj odročne lokacije, dokumentacija večje vrednosti v službenih vozilih, itd.), zaradi katerih naj navedenega ne bi bilo mogoče varovati na drugačen način. IP naj bi v pozivu navajal celo, da naj niti s sledenjem ne bi bilo mogoče gotovo varovati vseh situacij ogroženosti

(premoženja ali ljudi), pri čemer naj bi zavezanec štel, da je varnost zaposlenih vedno na prvem mestu, zaradi česar naj bi se zaposleni z uporabo GPS tehnologije strinjali. Zaposlene naj bi s tehnologijo, v skladu s 14. členom Splošne uredbe seznanjali redno, ustno in pisno, zaposleni pa naj bi podpisali izjavo o seznanitvi. V letu 2018 naj bi področje dodatno uredili s sprejetjem pravilnika, zaposlenim pa naj bi bili, v primeru kakršnihkoli vprašanj tudi na voljo za pojasnila. Na nameščeno opremo naj bi zaposlene izrecno opozarjale nalepke v oz. na vozilih, zato zavezanec šteje, da je v zvezi s tem izpolnil vse zakonske zahteve.

Zavezanec je navajal, da lokacijskih podatkov zaposlenih ne obdeluje oz. podatkov, ki jih GPS tehnologija hrani, ne uporablja. Z uporabo GPS naprav naj bi se obdelovali podatki o lokaciji službenega vozila (datum in ura), opravljeni poti ter registrski številki vozila, ki se shranjujejo v posebni aplikaciji, do katere ima dostop samo direktor zavezanca in z uporabo katere pa naj ne bi prihajalo do obdelave osebnih podatkov zaposlenih. Enaki podatki naj bi se zbirali in hranili v evidenci potnih nalogov, iz katerih naj bi bilo ravno tako razvidno, kakšno pot in kdaj je posamezni zaposleni opravil. Gola evidenca pa naj delodajalcu ne bi omogočala zagotavljanja varnosti delavcev in premoženja, saj delavcem ne bi omogočala nikakršnega varovanja njihovih pravic, niti pravočasnega ukrepanja, ki naj bi ga delodajalec poskušal zagotoviti z uporabo GPS tehnologije, saj mu drugačen način ne bi bil poznan. Potni nalogi naj bi predstavljali del Evidence osebnih podatkov uporabnikov službenih vozil in potnih nalogov ter naj bi se hranili v zaklenjeni omari v zaklenjeni pisarni, do katerih imajo dostop le pooblaščen osebe. Do GPS aplikacije naj bi zavezanec dostopal z računalniškim programom, nameščenim na računalniku direktorja. Neposredne povezave med evidencama naj ne bi bilo. Do obdelave osebnih podatkov naj bi lahko prišlo v primeru povezave uporabe vozila na določen dan s potnim nalogom za službeno pot, kar naj bi imeli evidentirano v Evidenci uporabe GPS tehnologije. Obdelava osebnih podatkov naj bi se tako izvedla izključno v posebej utemeljenih primerih (kazniva dejanja, varovanje ljudi in premoženja, pomoč pri prometni nesreči, škodni dogodki, itd.) oz. izključno takrat, ko bi bila uporaba osebnega podatka nujna in sorazmerna za zagotavljanje zakonitega interesa zavezanca, v nasprotnem primeru pa naj se povezava posameznika s podatki, ki jih generira sistem GPS sledenja, ne bi vršila. Glede na navedeno naj bi šlo za sorazmeren obseg obdelave osebnih podatkov, ki naj ne bi bil v škodo zaposlenih oz. posameznikov, ki vozijo službena vozila, saj naj bi se njihovi podatki (dejansko) obdelovali le v izjemnih, posebej utemeljenih primerih, ko bi bilo to neizogibno potrebno in cilja ne bi bilo mogoče doseči brez njihove obdelave oz. na drug način. Da zavezanec z GPS tehnologijo neposredno ne obdeluje osebnih podatkov zaposlenih in naj to tudi ne bi bil njegov namen naj bi izhajalo tudi iz v postopku priložene revizijske sledi izpisa podatkov ter pojasnila družbe _____. Podatki, ki se jih lahko pridobi s pomočjo tehnologije GPS naj bi se nanašali na vozila in ne na posameznike. Zavezanec je navedel, da slednji sicer so določljivi, a naj bi bili, ob vgrajenem varnostnem mehanizmu, ki neposredne povezave ne omogoča, ustrezno zaščiteni. Zavezanec je v svojem odgovoru ponovil tudi že podane navedbe v zvezi z dostopanjem do podatkov o GPS sledenju v aplikaciji. Zavezanec je v zvezi s tem navedel tudi, da občasno opravi pregled oz. vpogled v sistem, ki pa naj bi bil informativne narave in naj bi se z njim zolj preverilo delovanje GPS sistema. V obdobju od 1. 1. 2021 naj bi bilo na ta način v aplikacijo vpogledano dvakrat, s tem pa naj ne bi prišlo do nobene obdelave osebnih podatkov. Zavezanec je navedel, da ne drži ugotovitev IP, da podatke hrani v obliki, ki dopušča identifikacijo posameznika, saj naj bi bila za to potrebna aktivnost pooblaščen osebe, do katere pa naj bi prišlo zgolj izjemoma oz. sploh še ne. V zvezi z rokom hrambe je zavezanec navedel, da ga je določila družba _____ za delovanje svoje aplikacije in da zavezanec na to ni imel nobenega vpliva. Na navedeno družbo naj bi naslovili vprašanje v zvezi s skrajšanjem roka, vendar naj odgovora v zvezi s tem še ne bi prejeli. Do obdelave osebnih podatkov naj bi torej lahko prišlo izključno takrat, ko bi bila obdelava osebnega podatka nujna in zavarovanja ne bi bilo mogoče zagotoviti na drug način, o čemer naj bi zavezanec presodil v vsakem primeru posebej ter v zvezi s tem naredil tudi test zakonitega interesa, s katerim naj bi še posebej skrbno presodil, ali je vpogled v podatke v konkretnem primeru utemeljen in potreben in sicer na podlagi

točke f) prvega odstavka 6. člena Splošne uredbe in 48. člena ZDR-1, pri čemer naj bi bili zakoniti interesi, za katere si prizadevajo zlasti varnost in zaščita opreme in dokumentov, ki se nahajajo v vozilih, preprečevanje protipravnega odvzema vozil, varnost zaposlenih, določitev lokacije v primeru prometne nesreče, uveljavljanje in obramba morebitnih pravnih zahtevkov, ipd. Zavezanec se je skliceval na že predložena dokazila, ki jih je v svojem odgovoru tudi navedel.

V zvezi z izvajanjem videonadzora je zavezanec navedel, da so ugotovitve IP v zvezi s kamerami 1, 2, 5 in 6 pravilne, da pa se ne strinja z navedbami, ki se nanašajo na kamere št. 3, 4, 7, 8 in 9, saj naj bi tudi v zvezi s slednjimi podali odgovore na vsa zastavljena vprašanja ter izčrpno pojasnili, da se videonadzor izvaja zaradi enega izmed zakonsko določenih razlogov ter skladno z določili ZVOP-1. V zvezi z izpolnjevanjem zakonskih pogojev za izvajanje videonadzora je zavezanec poudaril, da videonadzor znotraj delovnih prostorov izvaja le v izjemnih primerih, kjer je to nujno potrebno za varnost ljudi (in podredno premoženja), da videonadzor izvaja le glede tistih delov prostorov, kjer je potrebno varovati ljudi in premoženje, da ne izvaja videonadzora v garderobnih ali sanitarnih prostorih in da so bili njegovi delavci pred začetkom izvajanja videonadzora o njegovem izvajanju pisno obveščeni. Zavezanec naj bi imel v podjetju nameščenih devet videokamer, ki so nameščene na vhodu/izhodu stavbe, na dvorišču (na mestu, kjer se hrani tudi material) in proizvodnji, kjer se nahajajo naprave in oprema večje vrednosti ter naprave, ki naj bi bile lahko izjemno nevarne za zdravje in življenje zaposlenih (fotografije naprav je zavezanec posredoval IP). V letu 2017 naj bi se zavezanec, zaradi varovanja ljudi in premoženja, odločil za postavitvev kamer in hkrati tudi senzorjev za alarmiranje požara in vloma, v skladu s tem pa naj bi bil izdelan in postavljen sistem požarnega javljanja in videonadzora, z namenom aktivne požarne varnosti in vloma, zaščite premoženja zavezanca, zaščite delavcev in obiskovalcev, zagotavljanja nadzora vstopa in izstopa v/iz službenih prostorov in ker naj bi zaradi narave dela obstajala možnost ogrožanja zaposlenih, slednjega pa naj na drug način ne bi bilo mogoče zagotoviti. Če bi prišlo do poškodbe ali celo izgube življenja zaposlenega naj bi zavezanec nosil težko breme odgovornosti, zato naj bi poskušal storiti vse, da zaposlenim zagotovi varnost in pravočasno detektira morebitno napačno delovanje opreme. S tem naj zavezanec ne bi nadziral zaposlenih, saj naj lokacija kamer tega ne bi omogočala. Izvajanje videonadzora na območju proizvodnje naj bi bilo ključno tudi za primer javljanja požarnega sistema, saj naj bi se namreč samo na ta način lahko zagotovil priklic gasilcev, varovanja ipd. V primeru sprožitve alarma naj bi sistem obvestilo o alarmu poslal družbi _____, sledenja pa naj bi direktorja zavezanca opozorila, da je prišlo do alarma. Direktor naj bi moral takoj preveriti, ali je potrebna intervencija in to sporočiti družbi _____ Hitro ukrepanje naj bi bilo v takih primerih nujno, omogočil pa naj bi ga lahko samo vpogled v posnetke nadzornih kamer, ki pokrivajo območja, na katerih so zdravju in življenju najbolj nevarne naprave oz. naprave, pri katerih lahko pride do požara. Drugačen način varovanja življenja in premoženja pri zavezancu ne bi bil mogoč oz. naj se z njim ne bi dalo zagotoviti varnosti, kakršno uspejo zagotavljati z videonadzorom strojev v proizvodnji. Zavezanec naj bi moral kot delodajalec v prvi vrsti zagotavljati varnost in zdravje pri delu. Opustitev te dolžnosti naj bi lahko pomenila kaznivo dejanje zavezanca (delodajalca) in njegovih odgovornih oseb. Pri tem naj bi šlo za preventivno ravnanje zavezanca, a glede na dobroto, ki jo pri tem varuje, šteje, da je takšen varovalni ukrep (glede na izpolnjevanje zakonskih pogojev) upravičen. Nadomestilo zanj naj bi lahko predstavljalo samo fizično varovanje, kar pa naj bi bilo, glede na naravo delovnega procesa pri zavezancu, nemogoče zagotoviti. S tem v zvezi naj ne bi držalo, da naj zavezanec ne bi preveril vseh možnosti zagotavljanja varnosti, saj naj bi o tem temeljito premislili in razpravljali, videonadzor pa izvedli izključno na mestih, kjer naj bi bilo to potrebno, kar naj bi dokazovalo tudi število kamer v prostorih zavezanca. Zgoraj navedeno naj bi izčrpno izhajalo iz obvestila zaposlenim o uvedbi videonadzora ter pravilnika o izvajanju videonadzora pri zavezancu. Z uvedbo videonadzora naj bi se strinjali tudi zaposleni, zato zavezanec šteje, da do posega v njihovo informacijsko zasebnost ni prišlo.

II. Navedba določb predpisov, na katere se opira odločba

Varstvo osebnih podatkov je ustavna pravica posameznika, saj Ustava Republike Slovenije (Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a, v nadaljevanju Ustava) v 38. členu določa, da je zagotovljeno varstvo osebnih podatkov in da je prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

V skladu s 1. točko 4. člena Splošne uredbe pomeni osebni podatek katero koli informacijo v zvezi z določenim ali določljivim posameznikom; določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika. V 2. točki 4. člena Splošne uredbe je obdelava osebnih podatkov opredeljena kot vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje.

Obdelava osebnih podatkov je na podlagi prvega odstavka člena 6 Splošne uredbe zakonita le in kolikor je izpolnjen vsaj eden od naslednjih pogojev:

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

V prvem odstavku člena 5 Splošne uredbe, ki ureja temeljna načela v zvezi z obdelavo osebnih podatkov je najprej določena zahteva, da so osebni podatki obdelani zakonito, pošteno in na pregleden način v zvezi s posameznikom, na katerega se ti podatki nanašajo. Osebni podatki morajo biti zbrani za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni (omejitev namena). Poleg tega morajo biti osebni podatki ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo (najmanjši obseg podatkov). Osebni podatki so lahko hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je to potrebno za namene, za katere se obdelujejo (omejitev shranjevanja). V skladu z drugim odstavkom člena 5 Splošne uredbe je upravljavec odgovoren za skladnost z načeli iz prvega odstavka tega člena in mora biti to skladnost tudi zmožen dokazati.

Splošna uredba po opredelitvi pravnih temeljev za obdelavo osebnih podatkov v členih 13 in 14 določa pravice posameznika do informacij, ki mu jih mora podati upravljavec osebnih podatkov pred ali ob začetku obdelave

njegovih osebnih podatkov. Člen 13 Splošne uredbe tako določa nabor informacij, ki jih mora upravljavec osebnih podatkov zagotoviti posamezniku, kadar se osebni podatki pridobijo od posameznika, na katerega se nanašajo osebni podatki, med drugim identiteto in kontaktne podatke upravljavca, namene in pravno podlago za obdelavo, uporabnike ali kategorije uporabnikov osebnih podatkov ter nadalje tudi obdobje hrambe osebnih podatkov, obstoj pravic posameznika, obstoj pravice do preklica privolitve, pravico do vložitve pritožbe pri nadzornem organu.

Zakon o delovnih razmerjih (Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS, 81/19, 203/20 – ZIUPOPDVE, 119/21 – ZČmIS-A, 202/21 – odl. US, 15/22 in 54/22 – ZUPŠ-1; v nadaljevanju ZDR-1) v 48. členu določa, da se lahko osebni podatki delavcev zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem.

Zasebni sektor lahko, v skladu s 75. členom ZVOP-1, izvaja **videonadzor dostopa v svoje službene oziroma poslovne prostore**, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Odločitev sprejme pooblaščen posameznik osebe zasebnega sektorja. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora. O izvajanju videonadzora je potrebno pisno obvestiti vse zaposlene v osebni zasebnega sektorja, ki opravljajo delo v nadzorovanem prostoru. **Videonadzor znotraj delovnih prostorov** se lahko izvaja le v izjemnih primerih, pod pogoji, ki jih določa 77. člen ZVOP-1 tj. kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi. Videonadzor se lahko izvaja le glede tistih delov prostorov, kjer je potrebno varovati naštete interese. Prepovedano je izvajati videonadzor v delovnih prostorih izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih. Zaposleni morajo biti pred začetkom izvajanja videonadzora delovnih prostorov vnaprej pisno obveščeni o njegovem izvajanju.

III. Razlogi, ki glede na ugotovljeno dejansko stanje narekujejo odločitev glede izvajanja GPS sledenja službenih vozil

IP je na podlagi ugotovitev inšpekcijskega ogleda in odgovorov zavezanca ter posredovane dokumentacije ugotovil, da zavezanec izvaja GPS sledenje osmih službenih vozil tj. vozil, ki jih njegovi zaposleni (predvsem delavci proizvodnje, ki odhajajo na teren in projektanti) uporabljajo za opravljanje svojih službenih del in nalog, pri čemer gre za dostavna vozila (kombije) in dostavna osebna vozila (ne pa tudi tovornjake). Tako sledenje zavezanec izvaja s pomočjo posebnega oddajnika v vozilu in posebne aplikacije, v kateri sistem kontinuirano beleži opravljeno pot vozila in te podatke tudi shranjuje. Ugotovljeno je bilo tudi, da zavezanec pri izvajanju GPS sledenja sodeluje z zunanjim izvajalcem družbo _____, na katero je prenesel določena opravila v zvezi z izvajanjem obravnavanega sledenja (podatki pridobljeni pri GPS sledenju službenih vozil se hranijo na strežniku družbe _____). Zavezanec je v svojem odgovoru navedel, da je zaposlene o izvajanju GPS sledenja vozil ustrezno obvestil in za to svojo trditev IP predložil tudi nekatere dokumente (primer obrazca, ki ga podpisše zaposleni). Ugotovljeno je bilo, da zavezanec sledenje službenih vozil uredil tudi v svojem Pravilniku o izvajanju GPS sledenja (v nadaljevanju Pravilnik).

IP je v postopku preučil navedbe zavezanca, s katerimi je ta utemeljeval uvedbo in izvajanje GPS sledenja službenih vozil, pravne podlage za izvajanje takega sledenja, namene, ki jih zavezanec pri tem zasleduje in druge okoliščine obravnavane obdelave osebnih podatkov zaposlenih.

V zvezi s tem je IP najprej ugotovil, da gre pri izvajanju GPS sledenja vozil, ki jih uporabljajo zaposleni pri zavezancu nedvomno za obdelavo osebnih podatkov posameznikov, ki vozila, ki se jih sledi upravljajo, saj je posameznik, ki je v določenem trenutku upravljal določeno vozilo, na podlagi podatkov, s katerimi razpolaga zavezanec, vedno določen ali vsaj določljiv. Z izvajanjem obravnavanega GPS sledenja tako nastaja posebna zbirka osebnih podatkov, ki vsebuje veliko količino lokacijskih podatkov zaposlenih posameznikov tj. podatkov kje točno (mikrolokacija) se je v določenem trenutku določen zaposleni s službenim vozilom nahajal in koliko časa. Zavezanec GPS sledenje zaposlenih izvaja na način, da podatke o njihovih lokacijah beleži in zbira kontinuirano, sistematično in avtomatizirano, tako da lahko za vsakega od njih ves čas uporabe vozila v službene namene, v vsakem trenutku preveri kje se posameznik z vozilom nahaja, zbrani podatki pa mu omogočajo tako ugotavljanje tudi za nazaj. V zvezi s tem je potrebno zavriniti navedbe, ki jih je v svojih izjavah navajal zavezanec in ki so navedeni tudi v njegovih internih dokumentih, ki jih je posredoval IP, da pri izvajanju GPS sledenja ne prihaja do obdelave osebnih podatkov oziroma da lokacijski podatki postanejo osebni podatki šele takrat, ko upravljavec v praksi dejansko ugotovi, na katerega njegovega zaposlenega se nanašajo. Iz zgoraj podane definicije osebnega podatka, kot jo podaja Splošna uredba namreč povsem jasno izhaja, da se za osebni podatek šteje tudi podatek, ki se nanaša na posameznika, ki je »zgolj« določljiv in ne samo na podatek, ki se nanaša na že določenega posameznika. V obravnavanem primeru je povsem jasno, da lahko zavezanec, na podlagi podatkov, s katerimi razpolaga, na relativno enostaven način določi zaposlenega, ki je v določenem času uporabljal službeno vozilo in na katerega se nanašajo lokacijski podatki, ki so bili pri tem zbrani z GPS sledenjem tega vozila, kar pomeni, da je tak posameznik za zavezanca brez dvoma določljiv. To še toliko bolj velja glede na okoliščino, da zavezanec ne razpolaga z velikim številom službenih vozil in da tako z GPS sledi zgolj osmim službenim vozilom, kar pomeni, da zavezanec kot delodajalec na relativno enostaven in hiter način ugotovi, kdo je v določenem času uporabljal določeno službeno vozilo. Da je zaposleni, na katerega se nanašajo z GPS sledenjem službenih vozil zbrani lokacijski podatki določljiv je v svojih odgovorih navajal tudi sam zavezanec, zato ni jasna njegova hkratna trditev, da z GPS sledenjem službenih vozil ne obdeluje osebnih podatkov zaposlenih. Da obdelavo podatkov, ki se nanašajo na določljivega posameznika (podatkov o tem kje se je zaposleni v določenem časovnem intervalu z določenim službenim vozilom gibal) predstavlja že zbiranje takih podatkov in ne šele njihova nadaljnja obdelava, kot je to v svojih odgovorih navajal zavezanec, izhaja že iz definicije 2. točke 4. člena Splošne uredbe, ki zbiranje osebnih podatkov izrecno navaja kot primer njihove obdelave.

Po ugotovitvi, na kakšen način zavezanec izvaja GPS sledenje službenih vozil je IP v postopku ugotavljal, ali obstaja ustrezna pravna podlaga za izvajanje GPS sledenja službenih vozil in zaposlenih, ko taka vozila uporabljajo, na način in v obsegu, kot ga izvaja zavezanec tj. ali za tako sledenje obstaja katera od pravnih podlag iz prvega odstavka člena 6 Splošne uredbe. IP je moral pri obravnavanem GPS sledenju službenih vozil med službenim časom preučiti dejansko stanje, kot izhaja iz navedb zavezanca in določb njegovih notranjih aktov ter glede na to ugotavljati ali je za tako sledenje, v konkretnem primeru podana katera od pravnih podlag iz Splošne uredbe.

Zavezanec se je v zvezi s pravno podlago za obdelavo osebnih podatkov zaposlenih, do katere prihaja v okviru obravnavanega GPS sledenja skliceval na izpolnjevanje pogojev iz točke f) prvega odstavka člena 6 Splošne uredbe tj. da je obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec in da nad takimi interesi ne prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki.

Kot zakoniti interes, ki ga z izvajanjem GPS sledenja želi uresničevati je zavezanec najprej navedel varstvo njegovega premoženja, pri čemer naj bi varoval sama službena vozila pa tudi opremo in dokumentacijo, ki naj bi se v vozilih nahajali. IP poudarja, da varstvo premoženja vsekakor predstavlja zakoniti interes, ki ga je mogoče zasledovati tudi s pomočjo GPS sledenja službenih vozil, vendar pa zavezanec v konkretnem primeru ni izkazal, da je izvajanje GPS sledenja, na način kot ga izvaja, za varstvo tega interesa primeren in potreben ukrep. Ugotovljeno je namreč bilo, da zavezanec GPS sledenje izvaja tudi med vožnjo oziroma v času, ko zaposleni upravlja službeno vozilo to pa je čas v katerem sta tako vozilo kot tudi oprema, ki se v njem prevaža in se želi varovati, pod neposrednim in stalnim nadzorom zaposlenega, saj je ta med vožnjo v vozilu nujno prisoten, zaradi česar tako vozilo kot oprema v tem času nista ogrožena pred morebitno odtujitvijo. Zato iz navedb zavezanca ni jasno, na kakšen način zavezanec s stalnim GPS sledenjem službenih vozil, v času ko so na poti in jih vozijo oziroma upravljajo zaposleni in so vozila pod njihovim neposrednim nadzorom, zagotavlja varstvo premoženja, ki ga je zavezanec navajal v postopku. IP je, glede na okoliščine, ki jih je navajal zavezanec prepričan, da bi bilo kot primeren ukrep (tj. ukrep s katerim se lahko učinkovito dosega zasledovani namen) v danem primeru mogoče opredeliti le izvajanje GPS sledenja na način, da bi ga voznik vklopil, ko bi vozilo parkiral, na lokaciji, kjer bi bilo to vozilo lahko ogroženo in ga zapustil ter ga ob vrnitvi v vozilo ponovno izklopil. Ob tem pa velja poudariti, da tudi takšno izvajanje GPS sledenja zavezancu ne bi prav v ničemer koristilo, če bi storilec vlomil v vozilo in iz njega odtujil varovano opremo in dokumentacijo. Tudi zavezanec je varovanje opreme in dokumentacije, ki se nahajata v vozilu zgolj navedel kot varovani dobrini, ni pa z ničemer pojasnil, na kakšen način bi se ju v primeru vloma v vozilo z GPS sledenjem službenih vozil sploh dalo zavarovati. IP je glede na navedeno, v zvezi z varstvom premoženja, kot zatrjevanim zakonitim interesom zavezanca ugotovil, da je zavezanec obstoj takega zakonitega interesa sicer vsaj delno izkazal, ni pa izkazal, da je GPS sledenje, na način in v obsegu kot ga izvaja zavezanec, primeren in potreben ukrep za njegovo uresničevanje. Hkrati pa je ugotovil tudi, da je GPS oddajnik v službenem vozilu lahko primeren ukrep, ki omogoča izsleditev takega vozila v primeru njegove odtujitve, vendar pa se mora ta uporabljati tako, da zaposleni GPS napravo vklopi, ko vozilo parkira, na lokaciji, kjer bi bilo to vozilo lahko ogroženo ter ga ob vrnitvi v vozilo in pred nadaljevanjem službene vožnje, ponovno izklopi. Zbiranje podatkov o lokaciji službenega vozila, ko je to parkirano na določenem mestu, kjer bi zaradi objektivnih okoliščin lahko bilo ogroženo tako, po oceni IP, predstavlja primeren ukrep za varovanje zakonitega interesa zavezanca (izsleditev nezakonito odtujenega vozila), ki je hkrati sorazmeren, saj ne predstavlja tako velikega posega v informacijsko zasebnost zaposlenih, da bi interesi ali temeljne pravice in svoboščine zaposlenih prevladale nad tem njegovim interesom. Ob tem je nujno poudariti, da se vklapljanje GPS oddajnika v službenem vozilu ne sme izvajati na način, da bi moral zaposleni tak oddajnik vklopiti ob vsakem parkiranju vozila, ampak mora za zbiranje lokacijskih podatkov in poseg v informacijsko zasebnost zaposlenih, obstajati takšna stopnja nevarnosti ogrožanja premoženja zavezanca (njegovega vozila), da odtehta poseg v ustavno pravico zaposlenih. Samo v primeru zadostno izkazane objektivne nevarnosti ogrožanja vozila na določeni lokaciji parkiranja bo namreč mogoče trditi, da interesi ali temeljne pravice in svoboščine posameznega zaposlenega ne prevladajo nad zakonitim interesom zavezanca po varovanju njegovega premoženja in izkazati izpolnjevanje pogoja iz točke f) prvega odstavka člena 6 Splošne uredbe. Okoliščine, v katerih je službeno vozilo ob parkiranju ogroženo do te mere, da je za njegovo varovanje dopustno tudi zbiranje lokacijskih podatkov mora jasno in objektivno opredeliti zavezanec in z njimi seznaniti zaposlene, ki GPS sledenja službena vozila uporabljajo ter jim v zvezi s tem dati ustrezna navodila.

Nadalje je zavezanec kot zakoniti interes, ki naj bi ga uresničeval z GPS sledenjem zaposlenih navedel varnost delavcev, ki naj bi bila v tem, da bi se v primeru prometne nesreče, če bi bilo to potrebno, ugotovilo kje se vozilo nahaja. IP je v zvezi s tem ugotovil, da je stalno in sistematično GPS sledenje službenih vozil z namenom, da bi se ob nekem izjemnem in malo verjetnem dogodku lahko ugotovilo, kje se vozilo nahaja

očitno nesorazmerno, saj relativno intenzivnega poseganja v ustavno pravico zaposlenih, do katerega z opisanim ukrepom vsakodnevno prihaja, ne more odtehtati morebitna, a malo verjetna potrebnost enega lokacijskega podatka, v primeru nepredvidenega a malo verjetnega dogodka v nedoločeni prihodnosti. Ob tem je nujno upoštevati tudi dejstvo, da tudi, če bi do nesreče službenega vozila prišlo, obstaja zelo majhna verjetnost, da bi bilo potrebno lociranje vozila s pomočjo sistema GPS, saj je kraj nesreče v veliki večini primerov znan in ga ni potrebno ugotavljati s pomočjo GPS lociranja vozila. Tudi, če bi se nesreča zgodila na odročnejšem kraju pa bi obvestilo o nesreči in lokacijo kjer se je zgodila lahko preko mobilnega telefona lahko sporočil voznik takega vozila. Ob tem je nujno pojasniti, da bi bilo v primeru prometne nesreče dopustno in zakonito tudi GPS lociranje službenega vozila na način, da bi zaposleni ob nesreči vklopil GPS napravo v vozilu, zavezanec pa bi za namene ukrepanja in zaščite zaposlenih potem prejel podatek o lokaciji, na kateri se nahaja ponesrečeno vozilo. IP je glede na navedeno, v zvezi z varstvom zaposlenih, kot zatrjevanim zakonitim interesom zavezanca ugotovil, da je zavezanec tudi obstoj takega zakonitega interesa sicer izkazal, vendar pa je bilo v zvezi s tem ugotovljeno, da bi bilo izvajanje GPS sledenja na način, kot ga izvaja zavezanec lahko pripomoglo k varovanju zaposlenih na zatrjevani način le v resnično izjemnih, hipotetičnih primerih, verjetnost nastanka katerih je minimalna poleg tega pa bi tudi v takih primerih zavezanec za doseg tega namena lahko uporabil tudi druga, v informacijsko zasebnost manj posegajoča sredstva pa tudi podatek o lokaciji službenega vozila, ki bi ga pridobil tako, da bi zaposleni ob nesreči vklopil sledenje GPS v vozilu in zavezancu poslal podatek o svoji lokaciji. Glede na navedeno je IP ugotovil, da zavezanec ni izkazal, da bi bila stalno in kontinuirano GPS sledenje službenim vozilom in obdelava osebnih podatkov, ki jo tak ukrep obsega, potrebna za doseganje namena varnosti zaposlenih v primeru prometnih nesreč, kot ga je predstavil zavezanec in s tem v skladu z določbo točke f) prvega odstavka člena 6 Splošne uredbe, saj lahko zavezanec ta namen v celoti doseže z zbiranjem in obdelavo neprimerljivo manjšega nabora lokacijskih podatkov (zgolj podatka o lokaciji prometne nesreče). GPS sledenje kot ga izvaja zavezanec je tudi v neskladju z načelom najmanjšega obsega podatkov iz točke c) prvega odstavka člena 5 Splošne uredbe, saj predstavlja zbiranje veliko večjega obsega podatkov, kot bi bilo potrebno za doseganje zgoraj navedenih dveh namenov, ki jih je v postopku navajal zavezanec.

Glede zakonitega interesa uveljavljanja in obrambe morebitnih pravnih zahtevkov, IP poudarja, da je zavezanec tak svoj interes v svojih vlogah v postopku zgolj omenil oziroma navedel, ni pa ga z ničemer konkretiziral in pojasnil, na kakšen način naj bi z GPS sledenjem službenih vozil, ki ga izvaja na ugotovljeni način tak namen lahko uresničeval (na kakšen način in zakaj naj bi bilo za doseganje tega namena potrebno sistematično in kontinuirano GPS sledenje službenih vozil, kot ga izvaja) ter ni izkazal sorazmernosti obdelave osebnih podatkov, do katere pri tem prihaja, čeprav bi to, v skladu z drugim odstavkom člena 5 Splošne uredbe moral izkazati in dokazati. Glede na navedeno zavezanec tudi glede navedenega interesa ni izkazal obstoja pogoja iz točke f) prvega odstavka člena 6 Splošne uredbe, na katerega se je v postopku skliceval.

Iz vsega zgoraj navedenega izhaja, da zavezanec z izvajanjem kontinuiranega, sistematičnega in avtomatiziranega GPS sledenja službenih vozil zbira in nadalje obdeluje lokacijske podatke vozil in voznikov (zaposlenih pri zavezancu), ki taka vozila upravljajo oziroma uporabljajo. Ker je vsak voznik določljiv posameznik tako zbrani lokacijski podatki predstavljajo tudi njegove osebne podatke, v smislu določb Splošne uredbe, za obdelavo katerih bi moral imeti zavezanec katero od pravnih podlag iz prvega odstavka člena 6 Splošne uredbe, obdelavo pa bi moral izvajati v skladu z načeli iz člena 5 Splošne uredbe. IP je v postopku inšpekcijskega nadzora, v skladu z zgoraj navedenim ugotovil, da zavezanec za obdelavo lokacijskih osebnih podatkov posameznikov, na v tem postopku ugotovljeni način ni izkazal obstoja katere od pravnih podlag iz prvega odstavka člena 6 Splošne uredbe (čeprav bi moral biti v skladu z drugim odstavkom člena 5 Splošne uredbe zmožen dokazati, da podatke obdeluje zakonito) in da obravnavana

obdelava lokacijskih podatkov ni v skladu z načelom najmanjšega obsega podatkov iz točke c) prvega odstavka člena 5 Splošne uredbe. V zvezi s tem je bilo ugotovljeno, da določenih namenov, ki jih je navajal zavezanec z uporabo GPS sledilnih naprav v službenih vozilih sploh ni mogoče doseči in zato obdelava lokacijskih podatkov za njihovo doseganje sploh ne more biti primerna in potrebna (GPS sledilne naprave v ničemer ne varujejo pred vlomom v službeno vozilo in odtujitvijo opreme in dokumentacije, ki se v vozilu nahaja), medtem ko bi take naprave za doseganje nekaterih drugih navedenih namenov lahko bile primerne in potrebne, če bi zavezanec lokacijske podatke z njimi zbiral in obdeloval v skladu z načelom najmanjšega obsega podatkov (GPS naprave lahko pripomorejo k izsleditvi ukradenega vozila, vendar za doseg tega namena zadošča vklop naprave ob parkiranju službenega vozila na določenem izpostavljenem, nevarnem mestu; GPS naprave bi v izjemnih, hipotetičnih primerih lahko bile potrebne za lociranje vozila ob prometni nesreči, vendar za doseg tega namena zadošča vklop naprave ob prometni nesreči). IP je v zvezi s tem ugotovil, da ugotovljena nepravilnost v času izdaje te odločbe še traja, saj zavezanec GPS sledenje na ugotovljen način še vedno izvaja in s tem še naprej ravna v nasprotju z omenjenimi določbami Splošne uredbe, zaradi česar je bilo potrebno odločiti, kot je razvidno iz 1. točke izreka te odločbe. Kot izhaja iz zgornjih pojasnil, bo zavezanec kljub tej prepovedi lahko lokacijske podatke službenih vozil zbiral tudi s pomočjo GPS naprav v teh vozilih, vendar ne sistematično in kontinuirano, ampak zgolj v omejenem obsegu in sicer tako, da bo lahko s temi napravami zbral podatke o lokacijah službenih vozil, ko bodo ta parkirana na mestih, kjer bo podana nevarnost njihove odtujitve in sicer na način, da zaposleni, ki vozilo uporablja, ob njegovem parkiranju tako GPS slednje vklopi, ko pa se v vozilo vrne pa ga izklopi. Prav tako bo v skladu z določbami Splošne uredbe dopustno GPS zbiranje lokacijskih podatkov v primeru prometne nesreče in sicer na način, da zaposleni ob nesreči vklopi GPS napravo in tako zavezancu omogoči ugotavljanje lokacije prometne nesreče.

Zavezanec je v postopku kot pravno podlago za izvajanje GPS sledenje službenih vozil navajal točko f) prvega odstavka člena 6 Splošne uredbe v povezavi z 48. členom ZDR-1, vendar pa je v svojih vlogah nato utemeljeval potrebnost take obdelave osebnih podatkov zgolj za različne (zgoraj navedene) zakonite interese v smislu navedene določbe Splošne uredbe, ni pa konkretiziral in pojasnil (razen glede varnosti zaposlenih v primeru prometnih nesreč) zakaj naj bi bilo tako sledenje potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem, za uresničevanje katerih njihovih pravic oziroma obveznosti naj bi bilo tako tako sledenje potrebno in zakaj njihovega uresničevanja ni mogoče zagotoviti z drugimi sredstvi in načini, s katerimi bi se v manjši meri posegalo v njihovo informacijsko zasebnost kot s stalnim in kontinuiranim sledenjem službenih vozil. Glede na navedeno zavezanec tudi ni izkazal obstoja pravne podlage iz 48. člena ZDR-1, na katero se je v postopku skliceval v povezavi z določbo točke f) prvega odstavka člena 6 Splošne uredbe, niti njenega obstoja v postopku ni ugotovil IP.

IP ob navedenem poudarja še, da ne drži trditve zavezanca, da pri GPS sledenju službenih vozil, kot ga izvaja, ne gre za sistematično in kontinuirano sledenje. Zavezanec te svoje trditve sicer ni v ničemer pojasnil, IP pa v zvezi s tem poudarja, da ne drži, saj zavezanec s sistemom GPS sledenja neselektivno sledi vsem službenim vožnjam, ki jih z osmimi službenimi vozili opravljajo njegovi zaposleni, poleg tega pa tem službenim vožnjam sledi neprekinjeno in v celoti.

Poleg navedenih nepravilnosti je IP v inšpekcijskem postopku ugotovil tudi, da zavezanec s tem, da lokacijske podatke službenih vozil, ki jih pridobi z njihovim GPS sledenjem v programu hranili še eno leto po tem, ko so bili zbrani, ravna v nasprotju z načelom omejitve shranjevanja osebnih podatkov iz točke e) prvega odstavka člena 5 Splošne uredbe, po katerem morajo biti osebni podatki hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za

namene, za katere se osebni podatki obdelujejo. Ker je IP zavezancu s to odločbo prepovedal izvajanje GPS sledenja službenih vozil na ugotovljeni način je omejevanje hrambe podatkov, ki jih je na ugotovljen način zbiral postalo brezpredmetno, saj zavezanec teh podatkov na tak način in v takem obsegu ne sme več zbirati. Kot je bilo pojasnjeno zgoraj pa je zavezanec v postopku izkazal obstoj dveh zakonitih interesov, za doseganje katerih bi lahko (v skladu z načelom sorazmernosti) zbiral tudi lokacijske podatke, s pomočjo GPS sledilnih naprav v službenih vozilih, v takem primeru pa bi moral tako zbrane podatke hraniti v skladu z načelom omejitve shranjevanja podatkov tj. zgolj toliko časa, kot je potrebno za dosego namenov, ki jih upravljavec s tako obdelavo zasleduje. Glede na zgoraj navedene uporabe GPS naprave, ki bi bile, glede na navedene okoliščine dopustne to pomeni, da bi lahko zavezanec podatke o lokaciji na nevarnem mestu parkiranega vozila hranil do takrat, ko nevarnost, zaradi katere se podatki zbirajo preneha, torej do takrat, ko zaposleni pride v vozilo in GPS sledenje izklopi, saj je takrat navedeni namen zbiranja teh podatkov (varovanje parkiranega vozila) izpolnjen in podatki niso več potrebni. Če pa bi dejansko prišlo do odtujitve službenega vozila pa bi zavezanec seveda lahko lokacijske podatke, ki bi jih v zvezi s takim dogodkom zbral z GPS napravo zavaroval in hranil tudi dlje časa, saj je za doseganje namena varovanja premoženja lahko potrebna njihova daljša hramba (npr. za uveljavljanje pravnih zahtevkov v uradnih postopkih). Enako velja tudi za uporabo GPS naprav za namene lociranja vozila v primeru prometne nesreče: namen takega zbiranja lokacijskih podatkov je izpolnjen, ko se s pomočjo tega podatka locira ponesrečeno vozilo in izvede ustrezna intervencija na kraju nesreče in takrat se morajo z GPS napravo zbrani lokacijski podatki pri zavezancu izbrisati. Če pa zavezanec v posameznem primeru izkaže, da je za doseganje zakonitega namena potrebna njihova daljša hramba (npr. za uveljavljanje pravnih zahtevkov v uradnih postopkih) pa lahko tudi tako zbrane podatke posebej zavaruje in hrani do izpolnitve tako izkazanega namena. IP je v zvezi s hrambo z GPS sledenjem službenih vozil zbranih lokacijskih podatkov ugotovil, da s tem povezana nepravilnost v času izdaje te odločbe še traja, da pa bo odpravljena že z izvršitvijo prve točke te odločbe in da za njeno odpravo zato zavezancu ni potrebno nalagati izvajanja dodatnih ukrepov za odpravo nepravilnosti. Se pa zavezanca ob tem opozarja, da mora v primeru uporabe GPS naprave na način, za katerega je bilo zgoraj pojasnjeno, da bi bil po Splošni uredbi dopusten, pri hrambi teh podatkov ravnati v skladu s načelom omejitve shranjevanja osebnih podatkov iz točke e) prvega odstavka člena 5 Splošne uredbe in poskrbeti, da bodo podatki, ko bo dosežen namen, ki ga zavezanec z njihovo obdelavo zasleduje, izbrisani.

V zvezi z navedbo zavezanca, da je rok hrambe z GPS sledenjem zbranih podatkov določila družba _____ in da sam na to ni imel nobenega vpliva IP opozarja, da je v skladu z drugim odstavkom 5. člena Splošne uredbe zavezanec, kot upravljavec tisti, ki je odgovoren za skladnost obdelave osebnih podatkov s temeljnimi načeli varstva osebnih podatkov iz prvega odstavka istega člena, med katerimi je tudi načelo omejitve njihovega shranjevanja, kar pomeni, da je zavezanec tisti, ki mora poskrbeti, da se bodo predmetni podatki obdelovali v skladu s tem (in drugimi) načeli. V okviru te odgovornosti mora poskrbeti za spoštovanje tega načela ne samo, ko te podatke obdeluje sam, ampak tudi, ko jih zaupa obdelovalcu, da jih obdeluje v njegovem imenu. Obdelovalec lahko, v skladu z določbo 28. člena Splošne uredbe osebne podatke obdeluje samo po dokumentiranih navodilih upravljavca in ne more sam določati roka hrambe osebnih podatkov, katerih upravljavec je zavezanec.

IV. Razlogi, ki glede na ugotovljeno dejansko stanje narekujejo odločitev glede izvajanja videonadzora

V zvezi z izvajanjem videonadzora je IP na podlagi odgovorov zavezanca in posredovane dokumentacije v postopku ugotovil, da zavezanec izvaja videonadzor z devetimi videokamerami, pri čemer štiri kamere izvaja videonadzor zunanjih in delno notranjih (vhodnih) delov svoje stavbe (zavezanec jih je v

odgovoru opredelil kot vhode/izhode v/iz stavbe podjetja), s petimi kamerami pa nadzira območja proizvodnje, na katerih se nahajajo delovni stroji in se odvija delovni proces pri zavezancu tj. delovne prostore. Zavezanec je v svojem odgovoru, kot namene, za katere izvaja videonadzor navajal nekatere od namenov iz 75. in 77. člena ZVOP-1.

Na podlagi navedb zavezanca, posredovanih dokumentov in zaslonskih slik zajema videokamer je IP ugotovil, da zavezanec videonadzor dostopa v službene in poslovne prostore izvaja s kamerami številka 1, 2, 5 in 6 in sicer za namene varnosti svojega premoženja, ki se nahaja na območjih dostopa in zaradi zagotavljanja nadzora vstopa ali izstopa iz teh prostorov. IP je glede teh videokamer ugotovil, da je zavezanec v postopku izkazal, da videonadzor z njimi potreben za navedena dva namena, ki sta določena v 75. členu ZVOP-1.

Na podlagi navedb zavezanca, posredovanih dokumentov in zaslonskih slik zajema videokamer je IP ugotovil, da zavezanec videonadzor delovnih prostorov izvaja s kamerami številka 3, 4, 7, 8 in 9 in da naj bi ga izvajal za namene varnosti ljudi in premoženja. Pri tem naj bi šlo za videonadzor proizvodnih in drugih delovnih prostorov, v katerih naj bi se nahajale naprave in oprema večje vrednosti in naprave, ki naj bi bile izjemno nevarne za zdravje in življenje zaposlenih. Varnost ljudi in premoženja naj bi se s tem videonadzorom varovalo tudi na način zagotavljanja aktivne požarne varnosti in vloma. IP poudarja, da ZVOP-1 v 77. členu za videonadzor delovnih prostorov določa relativno stroge pogoje, saj njegovo izvajanje dopušča zgolj v izjemnih primerih, ko je to nujno potrebno za varstvo taksativno naštetih pravnih dobrin ter tega namena ni mogoče doseči z milejšimi sredstvi. Zakonodajalec je torej ocenil, da videonadzor delovnih prostorov predstavlja relativno hud poseg v ustavno pravico posameznikov (zaposlenih) do varstva njihovih osebnih podatkov, zaradi česar je videonadzor teh prostorov dopustil le v izjemnih primerih ob strogih zakonskih omejitvah. V obravnavanem primeru je zavezanec navajal zgolj, da se v delovnih prostorih, v katerih izvaja videonadzor nahajajo naprave in oprema, ki naj bi bile večje vrednosti in naj bi hkrati predstavljale izjemno nevarnost za življenje in zdravje ljudi, nikjer pa take opreme in naprav ni konkretno opredelil, niti ni pojasnil kaj konkretno predstavlja izjemno nevarnost za življenje in zdravje ljudi ter v čem je za nevarnost tj. zakaj gre v obravnavanem primeru za tako izjemen primer, da bi bilo zaradi varstva navedenih pravnih dobrin dopustno posegati v informacijsko zasebnost zaposlenih tudi z videonadzorom njihovih delovnih prostorov, ki predstavlja relativno resen poseg v njihovo informacijsko zasebnost. Zavezanec se je torej na izjemnost primerov, zaradi katerih naj bi izvajal obravnavani videonadzor delovnih prostorov zgolj skliceval, nikjer pa take izjemnosti ni konkretiziral ali je kakorkoli utemeljil. Zavezanec tudi ni z ničemer izkazal, zakaj naj bi bil videonadzor teh prostorov nujno potreben in teh pravnih dobrin ne bi bilo mogoče učinkovito varovati na noben drug način in z nobenimi drugimi sredstvi, postopki in ukrepi. V postopku zavezanec (razen požarnega alarma) ni navedel nobenih drugih postopov in ukrepov, ki jih je preučil in izvedel za zavarovanje predmetnih pravnih dobrin in zakaj z njimi slednjih ni mogoče ustrezno zavarovati. IP ob tem poudarja, da ne drži navedba zavezanca, da je iz zaslonskih slik razvidno, da naj videonadzorni sistem ne bi omogočal določljivega pregledovanja posnetkov, saj so zaposleni, katerih delovne prostore se s tem videonadzorom snema, za zavezanca kot delodajalca, glede na zajem kamer in kvaliteto posnetka ter druge podatke, s katerimi razpolaga, nedvomno določljivi.

IP je v postopku inšpekcijskega nadzora, v skladu z zgoraj navedenim ugotovil, da zavezanec za izvajanje videonadzora delovnih prostorov iz prejšnjega odstavka, ki ga izvaja s kamerami številka 3, 4, 7, 8 in 9 ne izpolnjuje pogojev iz 77. člena ZVOP-1, saj v obravnavanem primeru niso podane okoliščine, ki bi kazale, da gre za izjemen primer v smislu prvega odstavka 77. člena ZVOP-1, prav tako pa niso bile ugotovljene okoliščine, iz katerih bi izhajalo, da je predmetni videonadzor nujno potreben in da ljudi in premoženja v delovnih prostorih ni mogoče varovati z milejšimi sredstvi. Zavezanec izpolnjevanja pogojev za zakonito

izvajanje videonadzora delovnih prostorov, kot jih določa 77. člen ZVOP-1 v postopku ni izkazal, čeprav bi moral biti, v skladu z načelom odgovornosti iz drugega odstavka člena 5 Splošne uredbe zmožen dokazati tudi skladnost z načelom zakonitosti iz prvega odstavka istega člena tj. dokazati, da osebne podatke obdeluje zakonito. IP je v zvezi z izvajanjem videonadzora delovnih prostorov ugotovil, da navedena nepravilnost v času izdaje te odločbe še traja, saj zavezanec videonadzor delovnih prostorov še vedno izvaja, ne da bi bili za to izpolnjeni pogoji iz 77. člena ZVOP-1 in s tem še naprej ravna v nasprotju z določbami tega člena ZVOP-1, zaradi česar je bilo potrebno odločiti, kot to izhaja iz 2. točke izreka te odločbe.

V zvezi z navedbami zavezanca, da naj bi z videonadzorom zagotavljal varnost zaposlenih tako, da z njim pravočasno detektira morebitno napačno delovanje opreme IP poudarja, da bi bilo morebitno napačno delovanje naprav in opreme v delovnih prostorih hipotetično mogoče ugotavljati tudi preko pregledovanja posnetkov videonadzornega sistema, vendar pa pregled teh posnetkov ni niti edini, niti najučinkovitejši način ugotavljanja navedenega napačnega delovanja naprav in opreme. Pravilno delovanje takih naprav in opreme je namreč v prvi vrsti potrebno zagotavljati in preverjati neposredno preko zaposlenih, ki jih uporabljajo ali z njimi upravljajo, preko zaposlenih, ki so pri zavezancu zadolženi za neposredno spremljanje in nadzor delovnega procesa, naprav in opreme in njihovega delovanja pa tudi preko sistema javljanja napak s strani samih naprav. Taki načini ugotavljanja morebitnega napačnega delovanja naprav in opreme z njihovim neposrednim pregledovanjem in nadzorom ter sistemom avtomatskega javljanja napak so tudi veliko učinkovitejši in zanesljivejši, saj je s pregledovanjem posnetkov mogoče zaznati le najbolj očitne nepravilnosti v delovanju, ni pa mogoče preveriti ustreznosti delovanja natančno in v celoti. Poleg tega velja poudariti, da imajo delovni stroji natančno predpisana pravila in postopke njihove uporabe in v tem okviru tudi izpostavljene in popisane tudi vse nevarnosti, ki lahko nastanejo pri njihovi nepravilni uporabi in določene varnostne ukrepe, ki jih je potrebno pri njihovi uporabi spoštovati. Nevarnosti, ki jih predstavlja delovanje posameznega delovnega stroja in varnostni postopki in ukrepi, ki jih morajo zaposleni pri delu z njimi izvajati, da do nesreč in poškodb ne bi prišlo so torej zavezancu v naprej znani, kar pomeni, da zavezanec lahko in mora zaposlene obveščati in opozarjati na pravilno uporabo delovnih strojev in izvajanje predpisanih varnostnih ukrepov pri njihovi uporabi. Zavezanec kot delodajalec je dolžan izvajanje varnostnih ukrepov s strani zaposlenih tudi ustrezno nadzirati. IP se v zvezi s tem strinja z navedbo zavezanca, da je kot delodajalec dolžan zagotavljati varnost in zdravje pri delu ter da te dolžnosti ne sme opustiti.

Neprepričljiva je navedba zavezanca, da je izvajanje videonadzora na območju proizvodnje ključno za primer javljanja požarnega sistema, ker naj bi bilo samo na ta način mogoče zagotoviti hitro ukrepanje. Zavezanec namreč ni pojasnil zakaj sistem javljanja požara, ki ga je vzpostavil prav za varstvo v primeru požara in ki sporoči oziroma javlja proženje požarnega alarma varnostni družbi zavezanca ne omogoča hitrega ukrepanja (priklica gasilcev, varovanja) tj. zakaj varnostna služba ob proženju alarma ne more ustrezno odreagirati in da je za hitro ukrepanje potrebno preverjanje dogajanja preko videonadzornega sistema s strani direktorja zavezanca. Poleg tega je postopek, kot ga je opisal zavezanec sestavljen iz kar nekaj korakov (sistem sporoči oziroma javlja proženje požarnega alarma varnostni družbi, varnostna družba proženje alarma sporoči direktorju zavezanca, direktor zavezanca vpogleda v videonadzorni sistem in preveri stanje na terenu, direktor zavezanca nato varnostni družbi sporoči, da je potrebna intervencija, varnostna družba ustrezno intervenira) in ukrepanje v primeru požara kvečjemu upočasneno, saj bi bilo to nedvomno hitrejše, če bi varnostna služba ustrezno ukrepala takoj ob proženju požarnega alarma. Iz navedb zavezanca v postopku torej izhaja, da hitro ukrepanje v primeru požara pri zavezancu zagotavlja požarni alarm in da za doseganje tega namena ni v ničemer potreben tudi videonadzor delovnih prostorov. Slednji v opisanem primeru lahko služi zgolj kot sredstvo za ugotavljanje lažnih alarmov in preklic

intervencije v takih primerih, nikakor pa ne kot sredstvo za zagotavljanje hitrega ukrepanja v primeru požara in posledičnega zavarovanja zavezančevega premoženja, saj je to v celoti zagotovljeno z vzpostavljenim požarnim alarmom. Glede na navedeno ni mogoče zaključiti niti, da je videonadzor delovnih prostorov, kot ga izvaja zavezanec, glede na navedene okoliščine primerno sredstvo za doseganje navedenega namena (hitro ukrepanje v primeru požara) še manj pa, da pri zavezancu ne obstajajo milejši ukrepi za preprečevanje požarne ogroženosti in ukrepanje v primeru požara, kot je izvajanje videonadzora delovnih prostorov (zavezanec nekatere od teh ukrepov že izvaja). IP navedenemu dodaja še, da zavezanec poleg tega v postopku ni izkazal, da bi šlo pri njem oziroma v videonadzorovanih prostorih za poseben, izjemen primer požarnega ogrožanja (v smislu izjemnega primera iz 77. člena ZVOP-1), saj ni nikjer konkretiziral zakaj in v čem je vir takega izjemnega požarnega ogrožanja.

Navedeno v prejšnjem odstavku velja tudi glede izvajanja videonadzora za namene varovanja pred vlomom v prostore zavezanca. V zvezi s slednjim IP dodatno poudarja, da je ob drugih sredstvih, s katerimi se lahko objekti zaščitijo pred vlomi (protivlomna zaščita vhodov v objekte, protivlomni alarmi, varovanje s strani varnostnih služb....) primerno sredstvo za tako zaščito tudi videonadzor, vendar pa ne videonadzor delovnih prostorov, ampak videonadzor dostopov v prostore zavezanca v smislu 75. člena ZVOP-1, ki je hkrati učinkovitejši, ker je usmerjen na dostope v objekte, torej na kritična območja, na katerih lahko pride do nezakonitih vstopov v objekte in tako zagotavlja učinkovitejšo preventivo (kamere, ki nadzirajo dostope so praviloma na zunaj vidne in s tem odvrčajo potencialne vlomilce), kakor tudi naknadno odkrivanje in prepoznavo vlomilcev (zaradi svoje usmerjenosti na kritična območja dostopov), hkrati pa v znatno manjši meri posega v informacijsko zasebnost zaposlenih kot videonadzor njihovih delovnih prostorov oziroma delovnih mest. Tudi v predmetnem postopku se videokamere, ki nadzirajo dostope v objekte zavezanca (kamere številka 1, 2, 5 in 6) niso izkazale kot sporne.

Iz navedenega torej izhaja, da lahko zavezanec enako stopnjo varstva ljudi in premoženja v delovnih prostorih zagotavlja tudi na druge načine, brez izvajanja videonadzora in intenzivnega poseganja v informacijsko zasebnost zaposlenih. Zato v postopku ni bilo mogoče ugotoviti, da namena varstva ljudi in premoženja, kot ga je v svojih vlogah opredelil zavezanec (tj. v smislu preprečevanja bodočih nesreč in poškodb, na podlagi rekonstrukcije preteklih s pomočjo vpogleda v posnetke videonadzora), zavezanec ne bi mogel doseči z nobenimi milejšimi sredstvi in da je za doseg tega cilja videonadzor ne samo potreben, ampak nujno potreben tj. da se namena ne da dosegati na noben drug način, ampak zgolj in samo z videonadzorom delovnih prostorov.

IV. Sklepno

Na podlagi vsega zgoraj navedenega je IP zaključil:

- da zavezanec s kontinuiranim in sistematičnim GPS sledenjem službenih vozil, kot je bilo ugotovljeno v tem postopku, ravna v nasprotju z načelom zakonitosti, saj tako sledenje izvaja, ne da bi bil za njegovo izvajanje izpolnjen kateri od pogojev iz prvega odstavka 6. člena Splošne uredbe in v nasprotju z načelom najmanjšega obsega podatkov iz točke c) prvega odstavka člena 5 Splošne uredbe, da zavezanec s tem ravna v nasprotju z navedenima določbama Splošne uredbe in da taka nepravilnost v času izdaje te odločbe še traja, zaradi česar je moral IP izdati predmetno odločbo in odločiti, kot izhaja iz 1. točke izreka te odločbe,
- da zavezanec z izvajanjem videonadzora proizvodnje - delovnih prostorov, ki ga izvaja s kamerami številka 3, 4, 7, 8 in 9 na v tem postopku ugotovljeni način, ravna v nasprotju s 77. členom ZVOP-1, saj tak videonadzor izvaja, ne da bi bilo zanj izpolnjeni pogoji iz tega člena ZVOP-1 in da taka

nepravilnost v času izdaje te odločbe še traja, zaradi česar je moral IP izdati predmetno odločbo in odločiti, kot izhaja iz 2. točke izreka te odločbe.

Zaradi ugotovljene nepravilnosti je bilo treba zavezancu na podlagi 2. in 8. člena ZInfP, 3. točke prvega odstavka 54. člena ZVOP-1, 57(1) in točke (f) člena 58(2) Splošne uredbe ter prvega odstavka 32. člena ZIN, odrediti, da preneha z obdelavo osebnih podatkov, do katere prihaja pri izvajanju GPS sledenja službenih vozil na ugotovljeni način in pri videonadzoru delovnih prostorov z zgoraj opredeljenimi videokamerami in s tem preneha z obdelavo osebnih podatkov, ki je v neskladju z določbami Splošne uredbe in ZVOP-1, in sicer na način, kot je določen v 1. in 2. točki izreka te odločbe.

Odredba v 3. točki, da je zavezanec po izvršitvi ukrepov iz 1. in 2. točke izreka te odločbe dolžan v roku 5 dni po njihovi izvršitvi pisno obvestiti IP, temelji na določbi petega odstavka 29. člena ZIN, ki določa, da mora zavezanec o odpravljenih nepravilnostih takoj obvestiti inšpektorja.

Na podlagi 118. člena ZUP se v odločbi odloči o stroških postopka; ker v tem postopku niso nastali posebni stroški, je tako odločeno v 3. točki izreka.

Ta odločba je izdana po uradni dolžnosti in je na podlagi 22. člena Zakona o upravnih taksah (Uradni list RS, št. 106/10 – UPB5, 14/15 – ZUUJFO, 84/15 – ZZelP-J in 32/16) takse prosta.

Pouk o pravnem sredstvu: Ta odločba je v upravnem postopku dokončna. Zoper njo v skladu z določbo 55. člena ZVOP-1 ni dovoljena pritožba, mogoč pa je upravni spor z vložitvijo tožbe na Upravno sodišče Republike Slovenije, Fajfarjeva 33, 1000 Ljubljana, v roku 30 dni od prejema te odločbe. Tožbo se vložijo pri pristojnem sodišču neposredno pisno ali pa se mu pošlje po pošti. Tožbi v najmanj dveh izvodih je potrebno priložiti to odločbo v izvorniku ali prepisu.

*Blaž Pavšič,
državni nadzornik
za varstvo osebnih podatkov*