Vošnjakova 1, p.p. 78, Ljubljana, Slovenija
Telefon: ++386 (0) 1 230 97 30
Faks: ++ 386 (0) 1 230 97 78
www.ip-rs.si

Številka: 0612-145/2008/9
Datum: 17.7.2008

Informacijski pooblaščenec izdaja po državnem nadzorniku za varstvo osebnih podatkov na podlagi 54. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07-UPB1, v nadaljevanju ZVOP-1), 32. člena Zakona o inšpekcijskem nadzoru (Uradni list RS, št. 43/07 - UPB1, v nadaljevanju ZIN) ter 2. in 8. člena Zakona o Informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A, v nadaljevanju ZInfP) v zadevi inšpekcijskega nadzora nad izvajanjem določb ZVOP-1 pri zavezancu Republika Slovenija, Ministrstvo za gospodarstvo, Urad za varstvo konkurence, Kotnikova 28/1, 1000 Ljubljana, ki ga zastopa direktor Jani Soršak, po uradni dolžnosti naslednjo

O D L O Č B O

I. Zavezancu Republika Slovenija, Ministrstvo za gospodarstvo, Urad za varstvo konkurence, Kotnikova 28/1, 1000 Ljubljana, **se prepoveduje vsakršno nadaljnje odpiranje, preimenovanje, spreminjanje, pregledovanje, kopiranje, izpisovanje, razkrivanje, posredovanje, širjenje ali drugo dajanje na razpolago ter uporabo vseh datotek vrste .nsf (Lotus Notes), .pst, .ost, .pab in .oab (vse Microsoft Exchange/Outlook) ter .dbx (Microsoft Outlook Express),** to je datotek, iz katerih so razvidna sporočila in stiki, ki so jih v nadaljevanju našteti posamezni zaposleni v družbah Poslovni sistem Mercator d.d., Spar Slovenija trgovsko podjetje d.o.o. in Engrotuš podjetje za trgovino d.d., vzpostavljali prek elektronske pošte, **in map z uporabniškimi profili spodaj naštetih posameznikov, to je map, ki se nahajajo v mapi »pogon:\\Documents and Settings\« in v mapi »pogon:\\Users\«. Prej navedene datoteke in mape se nahajajo na sledečih medijih,** ki jih je zavezanec dne 7. in 8. julija 2008 izdelal in pridobil v okviru vodenja postopka ugotavljanja usklajenega ravnanja oziroma omejevalnega sporazuma med prej navedenimi družbami:

a. *V Poslovnem sistemu Mercator:*
   - na kopijah trdih diskov osebnih računalnikov sledečih oseb: …….

b. *V Spar Slovenija d.o.o.:*
   - na kopiji omrežnega diskovnega polja SAN oziroma poštnega strežnika, na katerem se nahajajo datoteke uporabnikov (profili in uporabniški domači direktorij) in elektronska pošta družbe, kamor so bile prekopirane vse dostopne poštne datoteke poštnega strežnika Microsoft Exchange in datoteke iz domačih direktorijev podatkovnega strežnika ……. ter datoteke uporabniških profilov za uporabnike …… (dva profila);
   - na kopiji trdega diska prenosnega osebnega računalnika znamke Lenovo, model T61, ki ga je uporabljala ……..;
   - na trdem disku prenosnega osebnega računalnika znamke Lenovo, model X61, ki ga je uporabljal ……..;

c. *V Engrotuš podjetje za trgovino d.d.:*
   - na kopiji trdega diska mrežnega prehoda v strežniški sobi;

- na kopiji trdega diska delovne postaje ……;
- na kopiji trdega diska prenosnega osebnega računalnika ……;
- na kopiji trdega diska prenosnega osebnega računalnika ……..;
- na kopiji trdega diska delovne postaje ……;
- na trdem disku prenosnega osebnega računalnika ……;
- na varnostnih kopijah .pst datotek (datotek elektronske pošte) s strežnika Pluton za osebe: ……..

II. Prepoved iz I. točke izreka te odločbe se mora izvršiti v rok štiriindvajsetih ur od vročitve te odločbe zavezancu.

III. Zavezanec mora v roku štiriindvajsetih ur od vročitve te odločbe blokirati dostop do datotek in map iz I. točke izreka te odločbe, in sicer na ta način, da vsakega od zgoraj navedenih medijev ob prisotnosti državnega nadzornika za varstvo osebnih podatkov zapečati v posebno ovojnico, ki se shrani v kovinsko protivlomno in protipožarno omaro pri zavezancu.

IV. V roku petih dni od vročitve te odločbe mora zavezanec v prisotnosti državnega nadzornika na drug medij prenesti vse pridobljene podatke iz medijev, navedenih v 2. odstavku I. točke izreka te odločbe, ki niso predmet prepovedi iz 1. odstavka 1. točke izreka te odločbe, o čemer je potrebno narediti zapisnik, iz katerega morajo biti razvidni kraj in čas prenosa podatkov, vrsta medija, na katerega se podatki prenašajo, osebna imena in podpisi oseb, ki so sodelovale pri prenosu ter natančen popis vseh datotek in map, ki so se iz posameznega medija prenesle na drug medij. Po prenosu podatkov se v prisotnosti državnega nadzornika medije iz 2. odstavka I. točke izreka te odločbe ponovno zapečati.

V. V treh dneh po pravnomočno končanih postopkih, ki jih v predmetni zadevi, povezani z zaseženo dokumentacijo, vodi zavezanec, je potrebno zapečatene podatke, navedene v 1. odstavku I. točke izreka te odločbe, trajno uničiti.

VI. Posebni stroški v postopku niso zaznamovani.

O b r a z l o ž i t e v

1. Postopek inšpekcijskega nadzora

Informacijski pooblaščenec (v nadaljevanju Pooblaščenec) je bil dne 7.7.2008 po telefonu obveščen, da Urad za varstvo konkurence v okviru svojega nadzora v Poslovnem sistemu Mercator d.d. kopira celotne trde diske nekaterih osebnih računalnikov, na katerih se nahajajo tudi osebni podatki in osebna korespondenca zaposlenih, zaradi česar naj bi bila kršena prisilna zakonodaja s področja varstva osebnih podatkov, saj navedeni urad za tovrstne posege v zasebnost nima ustrezne pravne podlage. Pooblaščenec je takoj po prejemu navedenega obvestila zoper zavezanca - Republiko Slovenijo, Ministrstvo za gospodarstvo, Urad za varstvo konkurence, Kotnikova 28/1, 1000 Ljubljana (v nadaljevanju zavezanec ali UVK) - po uradni dolžnosti uvedel postopek inšpekcijskega nadzora nad izvajanjem določb ZVOP-1, ki ga je Pooblaščenec vodil pod številko 0612-145/2008.

Državni nadzornik za varstvo osebnih podatkov pri Pooblaščencu (v nadaljevanju nadzornik) je v zgoraj navedenem postopku inšpekcijskega nadzora ugotovil, da si je zavezanec dne 7.7.2008 in dne 8.7.2008 v okviru vodenja postopka ugotavljanja usklajenega ravnanja oziroma omejevalnega sporazuma med družbami Poslovni sistem Mercator d.d., Dunajska cesta 107, 1000 Ljubljana, Spar Slovenija trgovsko podjetje d.o.o. Letališka cesta 26, 1000 Ljubljana in Engrotuš podjetje za trgovino d.d., Cesta v Trnovlje 10 A, 3000 Celje, pridobil sledeče medije oz. nosilce podatkov:

a. *V Poslovnem sistemu Mercator:*
   - kopije trdih diskov osebnih računalnikov sledečih oseb: ……;

b. V Spar Slovenija d.o.o.:
   - kopijo omrežnega diskovnega polja SAN oziroma poštnega strežnika, na katerem se nahajajo datoteke uporabnikov (profili in uporabniški domači direktorij) in elektronska pošta družbe, kamor so bile prekopirane vse dostopne poštne datoteke poštnega strežnika Microsoft Exchange in datoteke iz domačih direktorijev podatkovnega strežnika ……. ter datoteke uporabniških profilov za ……. (dva profila);
   - kopijo trdega diska prenosnega osebnega računalnika znamke Lenovo, model T61, ki ga je uporabljala ……..;
   - trdi disk prenosnega osebnega računalnika znamke Lenovo, model X61, ki ga je uporabljal ……;

c. V Engrotuš podjetje za trgovino d.d.:
   - kopijo trdega diska mrežnega prehoda v strežniški sobi;
   - kopijo trdega diska delovne postaje ……;
   - kopijo trdega diska prenosnega osebnega računalnika …….;
   - kopijo trdega diska prenosnega osebnega računalnika ……..;
   - kopijo trdega diska delovne postaje ……;
   - kopijo trdega diska prenosnega osebnega računalnika ……..;
   - varnostne kopije .pst datotek (elektronske pošte) s strežnika Pluton za osebe: ……. .

Zgoraj navedene medije (kopije ter trdi disk osebnega računalnika) je zavezanec v času inšpekcijskega ogleda dne 10.7.2008 hranil zaklenjene in zapečatene v kovinski protivlomni in protipožarni omari, ki se nahaja v njegovih poslovnih prostorih.

Pooblaščena uradna oseba UVK za opravljanje preiskave v prostorih družbe Poslovni sistem Mercator d.d. je pri opravljanju inšpekcijskega nadzora dne 7.7.2008 izjavila, da jim pravno podlago za kopiranje računalniških diskov daje 2. odstavek 29. člena Zakona o preprečevanju omejevanja konkurence (Uradni list RS, št. 36/08, v nadaljevanju ZPOmK-1), ki v 3. alineji določa, da pooblaščene uradne osebe lahko odvzamejo ali pridobijo kopije ali izvlečke iz poslovnih knjig in druge dokumentacije v kakršni koli obliki z uporabo fotokopirnih sredstev ter računalniške opreme podjetja ali urada. Peta alineja jih nadalje pooblašča, da lahko zasežejo predmete ter poslovne knjige in drugo dokumentacijo za največ 20 delovnih dni. Na vprašanje nadzornika o tem, zakaj kopirajo celotne diske osebnih računalnikov, saj se na njih nahajajo tudi osebne zadeve in vsebina elektronske pošte posameznega zaposlenega, in ne zgolj poslovna dokumentacija ter kaj bodo storili s pridobljenimi kopijami in kako bodo podatke varovali, je pojasnila, da celotne diske kopirajo iz razloga, ker imajo v zakonu pooblastilo, da lahko

pregledujejo celotno dokumentacijo v kakršni koli obliki, ne glede na nosilec podatkov. UVK stoji na stališču, da se vsa dokumentacija, ki se nahaja v prostorih družbe, šteje kot poslovna dokumentacija, ne glede na nosilec, na katerem je zapisana. Kopije diskov bodo varno shranili v vrečke in zapečatili ter varovali v skladu z zakonom. Po dogovoru s pooblaščencem družbe Mercator bodo kopije diskov pregledovali v prisotnosti oseb, ki so uporabljali osebne računalnike ali njihovih pooblaščencev. Na izrecno vprašanje nadzornika o tem, za kakšne namene in na kakšni pravni podlagi so kopirali in nameravajo pregledovati tudi elektronsko pošto zaposlenih, je pojasnila, da jim takšno podlago daje 2. alineja 2. odstavka 29. člena ZPOmK-1, namen tega pa je vodenje upravnega postopka, ki ga je urad uvedel zoper zadevne družbe. Zakoniti zastopnik zavezanca v zvezi z navedeno izjavo pooblaščene osebe UVK v določenem roku, ki se je iztekel dne 12.7.2008, ni podal nobenih pripomb.

Direktor UVK je v postopku inšpekcijskega nadzora dne 10.7.2008 izjavil, da do pregleda kopiranih diskov sploh še ni prišlo. Če bo prišlo do pregledovanja kopiranih diskov, bo UVK to storil v okviru preiskave zgolj ob prisotnosti oseb, pri katerih so bili pridobljeni podatki. Navedene osebe bodo imele možnost, da vsaka zase samostojno, predhodno, še preden bi posamezni delavci urada dobili možnost vpogleda v pridobljene podatke, odstrani datoteke, za katere bo utemeljeno trdila, da so bodisi osebni podatki bodisi zasebne zadeve, ki se ne nanašajo na poslovanje preiskovanih trgovskih družb. Vendar bo to morala storiti na način, ki bo omogočil naknadno objektivno preverbo, ali gre res za osebne podatke oz. zasebne zadeve. UVK celo predlaga, da se navedeni ogled in izločitev podatkov opravi ob prisotnosti Informacijskega pooblaščenca, v kolikor se bodo s tem strinjali tudi imetniki teh podatkov. Ne glede na zgoraj navedeno pa bo UVK od navedenih oseb zahteval izročitev e-pošte, za katero UVK utemeljeno domneva, da ne gre za osebne podatke oz. osebne zadeve navedenih oseb. Izrecno je poudaril, da je do t.i. kopiranja trdih diskov ob soglasju imetnikov nosilca kopiranih digitalnih podatkov prišlo izključno z namenom zavarovanja dokazov; navedeno pomeni, da UVK do tega trenutka kopiranih podatkov sploh še ni pogledal ali kako drugače obdeloval, niti jih ni mogel pogledati ob samem kopiranju, saj so kopirani trdi diski še vedno zapečateni in shranjeni v kovinski protipožarni in protivlomni omari ter zaklenjeni. Enako velja tudi za IT forenzike, ki so kopiranje dejansko opravili. Alternativno predlaga, da Informacijski pooblaščenec, kolikor je to v skladu z njegovimi pooblastili, sam pregleda skopirane trde diske in sam izloči podatke, ki se nanašajo na zasebne zadeve, UVK pa izroči ostale vsebine, ki se nahajajo na skopiranih trdih diskih.

Zgoraj navedene ugotovitve in pojasnila zavezanca so razvidni iz zapisnikov o inšpekcijskem nadzoru št. 0612-145/2008/2 z dne 7.7.2008, št. 0612-145/2008/4 z dne 9.7.2008 ter št. 0612-145/2008/6 z dne 10.7.2008, ki jih je v postopku napisal nadzornik in na katere zavezanec ni podal nobenih pripomb.

Pooblaščenec je dne 16.7.2008 v zvezi s predmetno preiskavo, ki jo zavezanec vodi v okviru postopka ugotavljanja usklajenega ravnanja oziroma omejevalnega sporazuma med družbami Poslovni sistem Mercator d.d., Spar Slovenija trgovsko podjetje d.o.o. in Engrotuš podjetje za trgovino d.d., prejel še pisni predlog za izdajo ureditvene odločbe, v katerem prijavitelj predlaga, da Pooblaščenec prepove vso nadaljnjo obdelavo osebnih podatkov, ki so bili pridobljeni na podlagi izvoženih poštnih nabiralnikov in kopij nosilcev digitalnih podatkov ter odredi, da UVK zavezanec omenjene zbirke osebnih podatkov uniči.

2. Razlogi za izrek ukrepa oz. prepoved obdelave osebnih podatkov

2.1. Krovni zakon s področja varstva osebnih podatkov v RS je ZVOP-1. Po določbi 1. točke 6. člena ZVOP-1 je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, posameznik pa je skladno z 2. točko 6. člena ZVOP-1 »določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa«.

Osebni podatki se po določbah 1. odstavka 8. člena ZVOP-1 lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. V 2. odstavku 8. člena ZVOP-1 je nadalje določeno, da mora biti namen obdelave osebnih podatkov določen v zakonu, v primeru obdelave na podlagi osebne privolitve posameznika pa mora biti posameznik predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov.

Pravne podlage za obdelavo osebnih podatkov v javnem sektorju, kamor glede na določbe 22. točke 6. člena ZVOP-1 spada tudi zavezanec, so podrobneje določene v 9. členu ZVOP-1, ki določa:

(1) Osebni podatki v javnem sektorju se lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon. Z zakonom se lahko določi, da se določeni osebni podatki obdelujejo le na podlagi osebne privolitve posameznika.

(2) Nosilci javnih pooblastil lahko obdelujejo osebne podatke tudi na podlagi osebne privolitve posameznika brez podlage v zakonu, kadar ne gre za izvrševanje njihovih nalog kot nosilcev javnih pooblastil. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od zbirk osebnih podatkov, ki nastanejo na podlagi izvrševanja nalog nosilca javnih pooblastil.

(3) Ne glede na prvi odstavek tega člena se lahko v javnem sektorju obdelujejo osebni podatki posameznikov, ki so z javnim sektorjem sklenili pogodbo ali pa so na podlagi pobude posameznika z njim v fazi pogajanj za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna in primerna za izvedbo pogajanj za sklenitev pogodbe ali za izpolnjevanje pogodbe.

(4) Ne glede na prvi odstavek tega člena se lahko v javnem sektorju izjemoma obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo.

Obdelava osebnih podatkov je v 3. točki 6. člena ZVOP-1 definirana kot kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali, ki so pri ročni obdelavi zbirke osebnih podatkov namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali

drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje. Kot sredstva obdelave pa ista določba navaja, da je obdelava lahko ročna ali avtomatizirana.

Zbirka osebnih podatkov je v 5. točki 6. člena ZVOP-1 definirana kot vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.

2.2. Iz ugotovitev v postopku inšpekcijskega nadzora je razvidno, da mediji, ki si jih je zavezanec dne 7. in 8. julija 2008 izdelal in pridobil v okviru vodenja postopka ugotavljanja usklajenega ravnanja oziroma omejevalnega sporazuma med družbami Poslovni sistem Mercator d.d., Spar Slovenija trgovsko podjetje d.o.o. in Engrotuš podjetje za trgovino d.d., vsebujejo med drugim tudi podatke o stikih, ki so jih zaposleni v prej navedenih družbah (ti zaposleni so v izreku te odločbe poimensko navedeni) vzpostavljali prek elektronske pošte. Navedena ugotovitev je razvidna iz seznama pridobljenih kopij, ki so priloga zapisnika o inšpekcijskem nadzoru št. 0612-145/2008/6 z dne 10.7.2008. Nadzornik ugotavlja, da se osebni podatki pri uporabi elektronske pošte nahajajo v posameznih datotekah, ki jih ustvari določena programska oprema za delo z elektronsko pošto. Gre predvsem za datoteke, kjer se nahajajo elektronska sporočila, vnosi v koledar in osebni imeniki. Iz podatkov, ki so bili pridobljeni na UVK, nadzornik ugotavlja, da se prej navedeni podatki nahajajo v datotekah vrst .nsf (Lotus Notes), .pst, .ost, .pab in .oab (vse Microsoft Exchange/Outlook) ter .dbx (Microsoft Outlook Express). Ti podatki vključujejo prometne podatke o prejetih in poslanih elektronskih sporočilih (datum in ura, pošiljatelj, prejemnik oz. prejemniki, zadeva, naslov elektronske pošte), podatke o stikih v osebnem imeniku ter vnose v koledar, pri čemer je potrebno upoštevati, da sodobne rešitve za elektronsko pošto omogočajo enostavno kopiranje elektronskih sporočil neposredno v koledar. Prometni podatki o prejetih in poslanih elektronskih sporočilih, ki se nahajajo v prej navedenih datotekah (datum in ura, pošiljatelj, prejemnik oz. prejemniki, zadeva, naslov elektronske pošte), se nanašajo na točno določene posameznike, saj naslov službene elektronske pošte posameznika le tega točno določa, zaradi česar se takšni podatki po definiciji iz 1. in 2. točke 6. člena ZVOP-1 nedvomno štejejo kot osebni podatki.

Pri kopiranju celotne vsebine trdega diska se poleg podatkov o uporabi elektronske pošte skopirajo tudi podatki iz uporabniškega profila. Uporabniški profil uporabnika je shranjen v posebni mapi na trdem disku računalnika, v njem se pa hranijo podatki, ki jih je potrebno šteti za osebne podatke uporabnika, in sicer gre za **podatke, ki nastajajo ob uporabi svetovnega spleta** (angl. *world wide web*). Konkretneje se v to mapo shranjujejo podatki o obiskanih spletnih straneh (URL naslov spletne strani in čas obiska, angl. *history*), shranjene začasne internetne datoteke (angl. *temporary internet files*), piškotki (angl. *cookies*), priljubljene spletne strani (angl. *favorites*). Poleg teh podatkov se odvisno od nastavitev sistema v navedeni mapi hranijo tudi podatki, ki se nanašajo na uporabniške nastavitve (npr. bližnjice na namizju) in drugi podatki. Lokacija mape z uporabniškim profilom je odvisna od operacijskega sistema in se v okolju Windows praviloma nahaja na naslovu »pogon:\\Documents and Settings« ali »pogon:\users«.

Zgoraj navedeni podatki o uporabi svetovnega spleta se po določbah 1. in 2. točke 6. člena ZVOP-1 nedvomno štejejo kot osebni podatki. Takšno stališče je podala tudi **Delovna skupina za varstvo podatkov iz člena 29 Direktive 95/46/ES** v *Mnenju 1/2008 o vprašanjih varstva podatkov v zvezi z iskalniki* z dne 4. 4. 2008 (WP 148) in *Mnenju 4/2007 o pojmu* osebnih podatkov z dne 20. 6. 2007 (WP 136), v katerih je delovna skupina jasno zapisala, da je potrebno podatke o obiskanih spletnih straneh, piškotke in druge podatke, ki nastajajo pri uporabi svetovnega spleta in se nanašajo na določenega in določljivega posameznika, šteti za osebne podatke. Navedenih podatkov zagotovo ni moč šteti za podatke iz poslovnih knjig ali poslovne dokumentacije ali druge dokumentacije, zato je za njihovo obdelavo skladno z 8. členom ZVOP-1 potrebna ustrezna pravna podlaga, kar pa v predmetni zadevi ni 2. odstavek 29. člena ZPOmK-1.

2.3. Zavezanec je v konkretnem primeru državni organ, torej oseba javnega sektorja in lahko zato osebne podatke zaposlenih v družbah Poslovni sistem Mercator d.d., Spar Slovenija trgovsko podjetje d.o.o. in Engrotuš podjetje za trgovino d.d., obdeluje le v primeru, če za obdelavo njihovih osebnih podatkov obstaja katera izmed pravnih podlag, ki jih določa 9. člena ZVOP-1. Nadzornik pri presojanju pravnih podlag za obdelavo osebnih podatkov zaposlenih v prej navedenih družbah, ki se nahajajo na medijih, navedenih v izreku te odločbe, uvodoma ugotavlja, da se v obravnavanem primeru določbe 2., 3., in 4. odstavka 9. člena ZVOP-1 ne morejo šteti kot pravna podlaga, ki bi zavezanca pooblaščala za obdelavo osebnih podatkov, ki se nahajajo na prej navedenih medijih, zavezanec pa se na te določbe niti ne sklicuje. Določb 2. odstavka 9. člena ZVOP-1 v obravnavanem primeru ni mogoče šteti kot pravno podlago iz razloga, ker zavezanec ni nosilec javnih pooblastil, poleg tega pa gre v zadevi nedvomno za izvrševanje nalog zavezanca. Določb 3. odstavka 9. člena ZVOP-1 ni mogoče šteti kot pravno podlago iz razloga, ker zavezanec osebnih podatkov zaposlenih v zgoraj navedenih družbah ne obdeluje za namene izpolnjevanja pogodbe ali za namene izvedbe pogajanj za sklenitev pogodbe. Določb 4. odstavka 9. člena ZVOP-1 ni mogoče šteti kot pravno podlago iz razloga, ker niso izpolnjeni vsi pogoji iz te določbe, zlasti pogoj, da se s takšno obdelavo ne sme poseči v upravičen interes posameznika, na katerega se podatki nanašajo.

Iz zgoraj pojasnjenega izhaja, da bi zavezanec osebne podatke, ki se nahajajo na medijih, navedenih v izreku te odločbe, lahko obdeloval le v skladu z določbami 1. odstavka 9. člena ZVOP-1, to je v primeru, če bi obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določal zakon. Zavezanec lahko kot organ javnega sektorja skladno z določbami 1. odstavka 9. člena ZVOP-1 obdeluje osebne podatke na podlagi osebne privolitve posameznika le v primeru, če je z zakonom določeno, da se določeni osebni podatki obdelujejo le na podlagi osebne privolitve posameznika. V obravnavanem primeru ZPOmK-1 ne določa osebnih podatkov, ki bi jih zavezanec lahko obdeloval na podlagi osebne privolitve posameznika. Poleg tega je potrebno opozoriti, da ravnanja posameznika, ki je pod grožnjo denarne kazni zaradi oviranja preiskave izročil določene nosilce osebnih podatkov oziroma privolil v obdelavo določenih osebnih podatkov, nikakor ni mogoče šteti kot osebno privolitev posameznika, ki je v 14. točki 6. člena ZVOP-1 definirana **kot prostovoljna izjava volje** posameznika, da se lahko njegovi osebni podatki obdelujejo za določen namen.

Ob upoštevanju zgoraj navedenega nadzornik zaključuje, da lahko zavezanec osebne podatke, ki se nahajajo na v izreku te določbe navedenih medijih, skladno z določbami 8. in 9. člena ZVOP-1 obdeluje le v primeru, če ga za takšno obdelavo osebnih podatkov pooblašča zakon.

Pooblastila oseb, ki so zaposlene pri zavezancu in zanj opravljajo preiskavo ali pa za zavezanca opravljajo posamezna strokovna dela, so določena v ZPOmK-1. Kot izhaja iz ugotovitev v postopku inšpekcijskega nadzora, je zavezanec zgoraj navedene medije pridobil na podlagi 2. odstavka 29. člena ZPOmK-1, po katerem pooblaščene osebe zavezanca lahko:
– vstopijo in pregledajo prostore, zemljišča in prevozna sredstva (v nadaljnjem besedilu: prostori) na sedežu podjetij in na drugem kraju, na katerem podjetje samo ali drugo podjetje po njegovem pooblastilu opravlja dejavnost in posle, iz katerih izhaja verjetnost kršitve določb tega zakona ali 81. ali 82. člena Pogodbe o Evropski skupnosti;
– pregledujejo poslovne knjige in drugo dokumentacijo ne glede na nosilec, na katerem je zapisana oziroma shranjena;
– odvzamejo ali pridobijo kopije ali izvlečke iz poslovnih knjig in druge dokumentacije v kakršni koli obliki z uporabo fotokopirnih sredstev ter računalniške opreme podjetja ali urada. Če zaradi tehničnih razlogov ni mogoče narediti kopij z uporabo fotokopirnih sredstev ter računalniške opreme podjetja ali urada, lahko odnesejo poslovne knjige in drugo dokumentacijo za čas, potreben, da se naredijo kopije. O tem naredijo uradni zaznamek;
– zapečatijo vse poslovne prostore ter poslovne knjige in drugo dokumentacijo za čas trajanja preiskave in v obsegu, potrebnem za njeno izvedbo;
– zasežejo predmete ter poslovne knjige in drugo dokumentacijo za največ 20 delovnih dni;
– zahtevajo od katerega koli predstavnika ali predstavnice (v nadaljnjem besedilu: predstavnik) ali osebe zaposlene v podjetju ustno ali pisno pojasnilo dejstev ali dokumentov, ki se nanašajo na predmet ali namen preiskave, ter o tem sestavijo zapisnik. Če pooblaščena oseba zahteva pisno pojasnilo, določi rok, v katerem mora biti posredovano;
– opravijo druga dejanja, ki so v skladu z namenom preiskave.

Nadzornik ugotavlja, da navedeni člen ne predstavlja zadostne pravne podlage za kopiranje elektronske pošte posameznih zaposlenih, kot je to storil zavezanec, niti ne predstavlja zadostne pravne podlage za odpiranje, pregledovanje in uporabo osebnih podatkov, ki so sestavni del elektronske pošte. Kopiranje, odpiranje, pregledovanje in uporaba elektronske pošte posameznika pomeni poseg v njegovo zasebnost, in sicer v pravico do tajnosti pisem in drugih občil oz. t.i. komunikacijske zasebnosti. To pojavno obliko zasebnosti varuje Ustava RS v 37. členu.

Nadzornik še ugotavlja, da zgoraj navedeni člen tudi ne predstavlja pravne podlage za obdelavo osebnih podatkov, ki nastajajo pri uporabi svetovnega spleta in se nanašajo na določenega in določljivega posameznika, saj navedenih podatkov nedvomno ni moč šteti za podatke iz poslovnih knjig, poslovne dokumentacije in druge dokumentacije.

Ustava RS v drugem odstavku 37. člena opredeljuje pogoje dopustnega posega v tajnost pisem in drugih občil, kadar gre pri tem tudi za poseg v nedotakljivost človekove zasebnosti: 1) poseg je mogoč samo na podlagi določenega zakonskega pooblastila, 2) poseg mora *ex*

ante odobriti sodišče, 3) poseg mora biti časovno omejen, 4) poseg je dopusten, če je nujno za uvedbo ali potek kazenskega postopka ali za varnost države (Komentar U RS, str. 399).

V drugem odstavku tega člena je torej določeno, da samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Obseg zaščite komunikacijske zasebnosti iz 37. člena Ustave RS izhaja iz potrebe po varovanju zaupnosti razmerij, v katere pri sporočanju stopa posameznik, in ne iz določene vrste, statusa ali lastništva uporabljenega občila, komunikacijskega sredstva (Komentar Ustave Republike Slovenije / Lovro Šturm (urednik); [avtorji [komentarja] France Arhar … et al.]. Ljubljana: Fakulteta za podiplomske državne in evropske študije, 2002, v nadaljevanju: »Komentar U RS«, str. 392). 37. člen varuje zaupnost pisem in drugih občil, glede katerih posameznik utemeljeno pričakuje zasebnost; v tajnost pisem in drugih občil ni mogoče poseči takrat, ko bi bila s tem kršena nedotakljivost človekove zasebnosti (Komentar U RS, str. 394). To pravico zagotavlja tudi Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (Zakon o ratifikaciji konvencije s protokoli, Uradni list RS, mednarodne pogodbe, št. 7/94; v nadaljevanju: EKČP).

Na tem mestu je treba opozoriti na dvojno varstvo elektronske pošte. Dvojno varstvo pomeni, da so na ta način zbrani podatki varovani z določbami 37. in 38. člena Ustave RS. 37. člen varuje vsebino, 38. člen pa t.i. prometne podatke (e naslov, kdo je komu pisal in kdaj).

Pravica do komunikacijske zasebnosti obsega tajnost vseh vrst občil in s tem varuje tajnost komunikacije, ki je posredovana s katerimkoli komunikacijskim sredstvom. Namen tega varstva je v preprečevanju, da bi se kdorkoli seznanil z vsebino posredovanega sporočila. Prav tako pa ta pravica zagotavlja svobodo komuniciranja, ki se izraža kot svobodna odločitev posameznika o tem, komu in kako bo določeno sporočilo posredovano, iz česar izhajajo prepovedi nesorazmernih poseganj v posameznikovo odločitev, kako, kdaj in s kom bo komuniciral. Ključno za poseg v to pravico je, da je zakon, ki takšen poseg dovoljuje, posebej jasen in določen, da je delovanje državnih organov na njegovi podlagi predvidljivo. Določno je treba v zakonu opredeliti, kdaj je poseg nujen, ker dokazov ni mogoče pridobiti na drug način ali je to nesorazmerno težko. Po 2. odstavku 37. člena Ustave RS lahko samo zakon predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstva tajnosti pisem in drugih občil in nedotakljivosti človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.

Določba drugega odstavka 29. člena ZPOmK-1 ne konkretizira posega v pravico do komunikacijske zasebnosti, zato takšen poseg ni dovoljen. Določba namreč med pojavnimi oblikami možne preiskave ne določa izrecno tudi obdelave elektronske pošte. Vsakršen poseg v temeljno človekovo pravico mora biti v skladu z zahtevo po sorazmernosti in pravni določnosti, kot temeljnima prvinama pravne države in z zahtevo iz 2. člena Ustave RS: poseg v pravico do komunikacijske zasebnosti bi moral biti vnaprej določen tako, da bi omogočal predvidljivost situacij, v katerih je poseg dopusten in v kakšnem obsegu. Pooblastilo zavezanca, da lahko odvzame ali pridobi kopije ali izvlečke iz poslovnih knjig in druge dokumentacije v kakršni koli obliki z uporabo fotokopirnih sredstev ter računalniške opreme podjetja ali urada, ne vključuje tudi kopiranja datotek, ki vsebujejo elektronsko pošto

posameznika. Glede nujnosti določnosti v zakonu je pomembno stališče Ustavnega sodišča RS, ki je v odločbi U-I-152/03 ob presoji določbe Zakona o policiji, ki je urejal varnostno policijsko pooblastilo ugotavljanja identitete tudi po samem videzu določene osebe, zapisalo, da »izpodbijana določba zaradi svoje nedoločnosti (2. člen Ustave) ne prestane preizkusa sorazmernosti v ožjem pomenu in kot taka ne ustreza zahtevam po predvidljivosti. Okoliščine oziroma kriteriji, ki policistu omogočajo sklepanje, "da oseba vzbuja sum, da bo izvršila, izvršuje ali je izvršila prekršek ali kaznivo dejanje," so premalo določno opredeljene, zlasti ko gre za "videz" in za "zadrževanje na določenem kraju". Zato izpodbijana določba zaradi svoje nedoločnosti dopušča prekomerne posege v pravico do nedotakljivosti zasebnosti, varovano v 35. členu Ustave.«

Na tej podlagi nadzornik ocenjuje, da ne glede na to, da ZPOmK-1 ne opredeljuje pojmov poslovne knjige, dokumentacija in računalniška oprema podjetja, sama generalna klavzula, ki sicer omogoča zelo široka preiskovalna pooblastila zavezancu, ne more zadostovati tudi za poseg v komunikacijsko zasebnost. Napačna razlaga oziroma razlaga zakonskih norm v nasprotju z Ustavo bi namreč bila nezakonita v primeru, da in če obstaja jasna in nedvoumna z Ustavo skladna razlaga. Ustavnoskladna razlaga pooblastil zavezanca na podlagi ZPOmK-1 pri opravljanju preiskave po oceni nadzornika ne omogoča pridobivanja elektronske pošte posameznih zaposlenih.

Na tem mestu je potrebno omeniti tudi Uredbo Sveta (ES) št. 1/2003 z dne 16. Decembra 2002 o izvajanju pravil konkurence iz členov 81 in 82 Pogodbe, ki velja kot neposredno uporabno pravo Evropskih skupnosti (v nadaljevanju ES), po kateri so tudi organi, pristojni za konkurenco v državah članicah, torej tudi zavezanec v tej zadevi, pooblaščeni za uporabo prava Skupnosti (6. tč. Preambule k tej Uredbi). Pri tem pa ta uredba ne preprečuje državam članicam, da na svojem ozemlju izvajajo nacionalno zakonodajo, ki varuje druge pravne interese, pod pogojem, da je ta zakonodaja združljiva s splošnimi načeli in drugimi določbama prava Skupnosti (9. tč. Preambule) in je treba zagotoviti, da se informacije lahko uporabijo le, če so bile pridobljene na način, ki fizičnim osebam zagotavlja enako raven varstva pravic do obrambe, kakršno zagotavljajo nacionalna pravila sprejemnega organa (16. tč. Preambule). 37. tč. Preambule poudarja tudi, da ta uredba spoštuje temeljne pravice in upošteva načela, ki jih priznava zlasti Listina o temeljnih pravicah Evropske unije, zato je treba to uredbo razlagati in uporabljati ob upoštevanju teh pravic in načel, s tem pa tudi pravice do spoštovanja zasebnega in družinskega življenja, določene v 7. čl., po kateri ima vsakdo pravico do spoštovanja njegovega zasebnega in družinskega življenja, stanovanja in občevanja. V tej luči je potrebno tolmačiti določbo 12. čl. Uredbe, ki določa izmenjavo informacij med Komisijo in organi, pristojnimi za konkurenco v državah članicah, ki v tretjem odstavku določa, da se smejo informacije uporabiti kot dokazno sredstvo za odreditev sankcij zoper fizično osebo, (med drugim) kadar so bile informacije pridobljene na način, ki spoštuje enako raven varstva pravic do obrambe fizičnih oseb, kakor jo predvideva nacionalno pravo organa, ki informacije sprejema. V določbi 20. čl. Uredbe so določena podobna preiskovalna pooblastila kot v 29. čl. ZPOmK-1, pri čemer se v primeru, ko podjetje nasprotuje pregledu, predvideva sodelovanje države članice, pri čemer se lahko za to sodelovanje, ki po nacionalnih pravilih zahteva odobritev pravosodnega organa, vloži prošnja za tako odobritev. Spoštovanje nacionalnega prava države članice odreja tudi 22. čl., ki ureja preiskave, ki jih izvajajo organi, pristojni za konkurenco v državah članicah, saj lahko organ, pristojen za

konkurenco v državi članici, na svojem ozemlju opravlja vse preglede ali druge preiskovalne ukrepe na podlagi svojega nacionalnega prava, tudi ko to dela v imenu in za račun organa, ki je pristojen za konkurenco v drugi državi članici ali za Komisijo. Bistveno je, da uradniki organov, pristojnih za konkurenco v državah članicah, ki so odgovorni za vodenje teh pregledov, pa tudi tistih, ki so jih dovolili ali odredili sami, svoja pooblastila izvajajo v skladu s svojimi nacionalnimi predpisi, sama Uredba pa ne omogoča zaključka, da so takšni posegi dovoljeni na njeni podlagi. Nadzornik v tej zadevi ocenjuje, da nacionalni predpisi ne določajo in ne dovoljuje posega v elektronsko pošto zaposlenih v podjetjih, ki so preiskovana, iz razlogov, ki so bili že pojasnjeni.

2.4. V sklop posameznikove pravice do zasebnosti sodi tudi informacijska zasebnost, ki jo v Republiki Sloveniji opredeljuje 38. člen URS. Elektronska pošta oz. v njenem okviru podatki o prejetih in poslanih elektronskih sporočilih uživajo dvojno varstvo, in sicer varstvo tajnosti pisem in drugih občil po 37. členu URS in tudi varstvo osebnih podatkov po 38. členu URS.

Gre namreč za podatke, ki so tudi po svoji naravi takšni, da se z njihovim sporočanjem oziroma njihovo obdelavo posega v človekovo zasebnost. Krovni zakon s področja varstva osebnih podatkov v RS je ZVOP-1. Skladno z ZVOP-1 je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Posameznik pa je skladno z 2. točko 6. člena ZVOP-1 »določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa«. Podatki iz programske opreme, ki omogoča posredovanje elektronske pošte oz. podatke o naslovnikih in pošiljateljih elektronskih sporočil, vsebujejo tudi osebne podatke.

Ključni ustavnosodni test, ki ga je potrebno uporabiti pri ocenjevanju dopustnosti posega v pravico do zasebnosti na splošno in posebej glede tajnosti pisem in drugih občil v primerih, ki niso že vnaprej urejeni z zakonom, je, kot izhaja iz Komentarja U RS (stran 401), kriterij, ki ga je prvo uporabilo vrhovno sodišče ZDA – razumno pričakovanje zasebnosti (»*reasonable expectation of privacy*«). Pozneje se je sintagma »razumnega pričakovanja zasebnosti« pojavila tudi v judikaturi ESČP v primeru Halford v. Združeno kraljestvo (25. 6. 1997, Reports, 1997-III). V odločitvi iz leta 1997 je doktrino izrecno prevzelo tudi slovensko US (odl. US VI, 158). Ključna maksima ustavnega varovanja zasebnosti je, da pravo (ustava) ne ščiti zgolj prostorov, lastnine ali lastnikov, temveč posameznike, ki v določenem trenutku, v določenem prostoru ali pri določenem ravnanju (upravičeno) pričakujejo svojo zasebnost.

Takšen poseg bi bil lahko izveden le pod v ustavi določenimi pogoji, kar primarno pomeni, da lahko samo zakon predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstva tajnosti pisem in drugih občil in nedotakljivosti človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.

Bistveno je, da posameznik (pošiljatelj ali sprejemnik sporočila) pri svojem ravnanju upravičeno pričakuje zasebnost. Poseg v omenjeno pravico je v odsotnosti izpolnjenih

pogojev iz 2. odstavka 37. člena prepovedan vsem, na prvem mestu pa državi, ter tudi posameznikom (Komentar U RS, str. 398). Pojem zasebno življenje vsebuje tako zasebno kot tudi službeno elektronsko pošto na službenem računalniku. To varstvo je priznano vsem osebam, saj U RS ne razlikuje med zasebnostjo v zasebni ali službeni sferi.

2.5. ZPOmK-1 sicer izrecno v 32. čl. iz preiskave izključuje t. i. privilegirano komunikacijo, po kateri so iz preiskave izključena pisma, obvestila ali drugi načini komunikacije med podjetjem, zoper katero se izvaja preiskava, in njegovim odvetnikom v obsegu, v katerem se nanašajo na ta postopek (v nadaljnjem besedilu: privilegirana komunikacija). Ta določba pa je odraz zaupnega razmerja med stranko (pravno osebo v tem primeru) in odvetnikom in temelji na maksimi, po kateri so pravila o izjemah od dolžnosti pričanja izraz spoznanja, da so nekateri interesi pomembnejši od interesa, da se ugotovi resnica (o tem več: Dragica Wedam Lukić, Varstvo osebnih podatkov v civilnih sodnih postopkih, Podjetje in delo 5-6/1996, str. 914-921). Vendar pa navedena določba ne dopušča sklepanja, da so *argumentum a contrario* komunikacije med drugimi osebami nezaščitene oz. podvržene preiskavi v skladu z drugim odstavkom 29. čl. ZPOmK-1. Sklepanje po nasprotnem razlogovanju je intepretacijsko pravilo, ki izhaja iz logične razlage in prepoveduje tako razlago posameznega jezikovnega znaka, s katero bi raztegnili njegov pomen tudi na druge subjekte, ki niso izrecno opredeljeni v posamezni določbi pravnega akta ter tudi od njih terjali ali jim dopuščali določeno ravnanje. Nadzornik na tem mestu ocenjuje, da uporaba tega sklepanja v tem primeru ni dopustna, ker hkrati predstavlja tudi zakonsko analogijo oz. *analogio legis*. Zakonska analogija naj bi sodila predvsem na področje logične razlage in omogoča uporabo določene norme tudi na druge, vnaprej nedoločene, vendar urejenemu zakonskemu dejanskemu stanu podobne primere. Pri zakonski analogiji gre torej za to, da primer, ki terja pravno rešitev, a je iz pravnih določb ni mogoče neposredno ugotoviti, uporabimo pravno normo, ki ureja podoben, analogen primer. Kadar govorimo o ustavnih temeljnih človekovih pravicah, je takšna zakonska analogija načeloma nedopustna. Zakonska analogija pa tudi uporaba splošnih pravnih načel v primeru pravnih praznin sta možni tako tedaj, ko ju je zakonodajalec izrecno predvidel in tudi tedaj, ko v okviru pozitivnega prava ni izrecnih določb o dopustnosti uporabe teh razlagalnih prijemov. Seveda pa lahko zakonodajalec izrecno prepove njuno uporabo na vseh tistih področjih, kjer prevlada spoznanje, da so pravna varnost, predvidljivost ter **zlasti še spoštovanje človekovih pravic**, še posebej tehtne vrednote, ki se jim mora podrediti tudi načelo popolnosti pravnega sistema ter v določeni meri tudi načelo njihove učinkovitosti (več Kušej, Pavčnik, Perenič: Uvod v pravoznanstvo, ČZP UL RS, Ljubljana, 1992, str. 209-210). Pravico do tajnosti in drugih občil torej v tem primeru terja določenost v zakonu in ne dopušča sklepanja po nasprotnem razlogovanju.

2.6. Nadzornik, ki pri opravljanju inšpekcijskega nadzora ugotovi kršitev ZVOP-1 ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, ima pravico takoj: odrediti, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovi, odpravijo na način in v roku, ki ga sam določi (1. točka prvega odstavka 54. člena ZVOP-1); odrediti prepoved obdelave osebnih podatkov osebam javnega ali zasebnega sektorja, ki niso zagotovile ali ne izvajajo ukrepov in postopkov za zavarovanje osebnih podatkov (2. točka prvega odstavka 54. člena ZVOP-1); odrediti prepoved obdelave osebnih podatkov ter anonimiziranje, blokiranje, brisanje ali uničenje

osebnih podatkov, kadar ugotovi, da se osebni podatki obdelujejo v nasprotju z določbami zakona (3. točka prvega odstavka 54. člena ZVOP-1); odrediti prepoved iznosa osebnih podatkov v tretjo državo ali njihovega posredovanja tujim uporabnikom osebnih podatkov, če se iznašajo ali posredujejo v nasprotju z določbami zakona ali obvezujoče mednarodne pogodbe (4. točka prvega odstavka 54. člena ZVOP-1); odrediti druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek (5. točka prvega odstavka 54. člena ZVOP-1).

Nadzornik ob upoštevanju zgoraj obrazloženega zaključuje, da zavezanec v obravnavanem primeru nima pravne podlage za obdelavo osebnih podatkov, ki se nanašajo na elektronsko pošto zaposlenih v družbah Poslovni sistem Mercator d.d., Spar Slovenija trgovsko podjetje d.o.o. in Engrotuš podjetje za trgovino d.d. ter se nahajajo na medijih, ki jih je zavezanec izdelal in pridobil v okviru vodenja postopka ugotavljanja usklajenega ravnanja oziroma omejevalnega sporazuma med prej navedenimi družbami ter da zavezanec nima pravne podlage za obdelavo osebnih podatkov, ki nastajajo pri uporabi svetovnega spleta in se nanašajo na določenega in določljivega posameznika. Nadzornik se je v konkretnem primeru odločil za izrek ukrepa prepovedi nadaljnje obdelave osebnih podatkov ter s tem povezan izrek ukrepa blokiranja nezakonito pridobljenih osebnih podatkov, zaradi načela sorazmernosti, ki ga določa 7. člen ZIN. Blokiranje podatkov po določbi 17. točke 6. člena ZVOP-1 pomeni takšno označitev osebnih podatkov, da se omeji ali prepreči njihova nadaljnja obdelava. Strožji ukrep (takojšnje uničenje nezakonito pridobljenih osebnih podatkov) bi lahko pomenil nepovraten poseg v celotno pridobljeno elektronsko dokumentacijo, saj bi takojšnje uničenje pridobljenih dokazov (uničenje še pred pravnomočno končanim postopkom, ki ga v predmetni zadevi vodi zavezanec) lahko izničilo pridobljeno gradivo kot relevanten dokaz. Glede na to, da je zavezanec dokumentacijo pridobil v okviru preiskave po ZPOmK-1, nepovraten poseg v celotno pridobljeno elektronsko dokumentacijo po pravnomočno končanem postopku pri zavezancu ne more več predstavljati izničenja pridobljenega gradiva, zato je nadzornik v V. točki izreka odredil uničenje nezakonito pridobljenih osebnih podatkov šele v treh dneh po pravnomočno končanih postopkih, ki jih vodi zavezanec v predmetni zadevi in so povezani z zaseženo dokumentacijo.

Ob upoštevanju zgoraj navedenega je bilo zavezancu na podlagi 3. točke 1. odstavka 54. člena ZVOP-1 ter 32. člena ZIN potrebno odrediti prepoved nadaljnje obdelave osebnih podatkov ter njihovo blokiranje in uničenje na način, kot je določen v izreku te odločbe.

Ta odločba je izdana po uradni dolžnosti in je na podlagi 22. členu Zakona o upravnih taksah (ZUT; Uradni list RS, št 42/07-UPB3 in 126/07) takse prosta.

Pouk o pravnem sredstvu:
Ta odločba je v upravnem postopku dokončna. Zoper njo po določbah 55. člena ZVOP-1 pritožba ni dovoljena, dovoljen pa je upravni spor z vložitvijo tožbe na Upravno sodišče Republike Slovenije, Fajfarjeva 33, 1000 Ljubljana, v roku 30 dni po prejemu te odločbe. Tožba se lahko pošlje priporočeno po pošti, ali poda pisno ali ustno na zapisnik neposredno pri

navedenem sodišču. Tožbi v dveh izvodih je treba priložiti to odločbo v izvirniku ali neoverjeno kopijo.

Jože BOGATAJ,
državni nadzornik
za varstvo osebnih podatkov

Vročiti:

- Republika Slovenija, Ministrstvo za gospodarstvo, Urad za varstvo konkurence, Kotnikova 28/1, 1000 Ljubljana, z vročilnico;
- arhiv, tu.