



Številka:

Datum:

USTAVNO SODIŠČE REPUBLIKE SLOVENIJE

Beethovnova 10

1000 Ljubljana

Informacijski pooblaščenec na podlagi 23.a čl. Zakona o Ustavnem sodišču (Ur. l. RS, št. 51/07 – ZUstS-A) vlaga v zvezi z zadevo inšpekcijskega nadzora, ki ga vodi pod št. 0613-1/2008, naslednjo

ZAHTEVO ZA OCENO USTAVNOSTI IN ZAKONITOSTI

3. in 4. odst. 390. čl. Zakona o bančništvu (Ur. l. RS, št. 131/2006 in 1/2008, ZBan-1):

"(3) Vse banke morajo, ne glede na to, ali so članice bančnega interesnega združenja, organizirati sistem izmenjave informacij o boniteti strank, ki so fizične osebe, med bankami iz 4. točke drugega odstavka 215. člena tega zakona. Ta sistem lahko za banke organizira tudi bančno interesno združenje.

(4) Banke morajo v sistem iz tretjega odstavka tega člena posredovati informacije o boniteti svojih strank."

* * *

O b r a z l o ž i t e v:

Izpodbijane določbe ZBan-1 so po oceni vlagatelja zahteve v neskladju z 38. čl. Ustave – določenost vrste osebnih podatkov.

Človekove pravice in temeljne svoboščine, med katere sodi tudi varstvo osebnih podatkov, so izhodiščni in osrednji del Ustave. Določba drugega odstavka 38. čl. Ustave RS določa, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov, ureja zakon. Varstvo osebnih podatkov je v Republiki Sloveniji ustavno zagotovljena človekova pravica, ki spada v okvir pravic s področja zasebnosti. Iz te ustavne določbe izhaja, da je zagotovljeno varstvo osebnih podatkov, uporaba v nasprotju z namenom njihovega zbiranja pa je prepovedana. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov, določa zakon. Z ustavo je zagotovljena tudi pravica posameznika do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj (lastni osebni podatki), kot tudi pravica do sodnega varstva ob zlorabi osebnih podatkov posameznika. Iz zgoraj citiranega 38. člena Ustave RS je razvidno, da se je ustavodajalec odločil za t.i. "obdelovalni model" v

nasprotju s t.i. "modelom zlorabe ". Za obdelovalni model je značilno, da so v zakonu določena pravila za urejanje takšne obdelave osebnih podatkov, ki je dopustna oziroma zakonita. Obenem to pomeni, da v pravnem redu Republike Slovenije ni načelne svobode pri obdelavi osebnih podatkov. Obdelovalni model izhaja iz premise, da je na področju obdelave osebnih podatkov prepovedano vse, razen tistega, kar je z zakonom izrecno dovoljeno. Vsaka obdelava osebnih podatkov namreč pomeni poseg v ustavno človekovo pravico do varstva osebnih podatkov. Poseg v to pravico pa je dopusten le, če je v zakonu natančno in določno opredeljeno, kateri osebni podatki se smejo obdelovati in v kakšen namen se smejo obdelovati. Pri tem mora biti namen obdelave osebnih podatkov ustavno dopusten, pri obdelavi osebnih podatkov pa se mora spoštovati načelo sorazmernosti tako, da se smejo obdelovati le tisti osebni podatki, ki so primerni in nujno potrebni za uresničitev zakonsko opredeljenega namena. Pri varstvu osebnih podatkov torej ni mogoče izhajati iz premise, da je dovoljeno vse, kar ni izrecno prepovedano.

Načelo zakonitosti primarno pomeni, da morajo biti splošna pravila obdelave osebnih podatkov predpisana z zakonom (tudi in predvsem z vidika *lex certa*), hkrati pa morajo vsi, ki obdelujejo osebne podatke, ravnati pošteno. Zakonitost obdelave osebnih podatkov pomeni, da se osebne podatke v Republiki Sloveniji lahko obdeluje le v skladu z zakonom oziroma na podlagi splošnega pooblastila iz zakona. Na področju varstva osebnih podatkov je treba drugi odstavek 38. člena Ustave razumeti tako, da se pravice in obveznosti upravljavcev osebnih podatkov lahko določajo zgolj z zakonom.

Področje varstva osebnih podatkov je tako primarno prepuščeno zakonskemu urejanju. O tej zakonodajalčevi skrbi in dolžnosti je odločalo že Evropsko sodišče za človekove pravice (ESČP), ko je v primeru *Narinem proti Finski* ugotovilo kršitev 8. člena EKČP in zapisalo, da za dopustno obdelavo osebnih podatkov ne zadostuje le določenost v zakonu, pač pa mora biti tudi sam zakon »v skladu z vladavino prava, to pomeni, da mora biti zakon kakovosten«. Primarno vprašanje v tem primeru je bilo, ali konkreten ukrep posega v zasebnost v skladu z zakonom, torej v mejah, ki jih postavlja zakon. Vendar pa je sodišče v svoji obrazložitvi zapisalo, da je pri tem pomembna tudi sama kakovost tega zakona in torej ne zadošča zgolj dejstvo, da zakon obstaja. To pomeni, da mora biti zakon skladen z vladavino prava, načeli pravne države torej, posamezniku pa mora omogočiti predvideti posledice zanj. Četudi se je v konkretnem primeru tožena stranka sklicevala na zakonsko pravno podlago za obdelavo osebnih podatkov, je ESČP ugotovilo, da so zakonska določila presplošna in da zaradi svoje nedoločnosti ne dajejo ustreznega varstva.

Negativna dolžnost države po 8 čl. EKČP, da se vzdrži poseganja v zasebnost, posamezniku zagotavlja varstvo pred samovoljo javnih oblasti. Pravica do zasebnosti je pravica do lastnega življenja s čim manj vmešavanji in vključuje svobodo posameznika pred neutemeljenimi posegi države v njegovo zasebno sfero (*right to be let alone*). V sodbi *Malone proti Združenemu kraljestvu* z dne 2.8.1984, A 82, je ESČP obravnavalo predvsem vprašanje **določenosti z zakonom** in vsebino zahteve »v skladu z zakonom«. Sodišče je v tem primeru ocenilo, da zakonodaja ne dolga dovolj jasno, kdaj in kako so dovoljeni ukrepi prisluškovanja, ki tudi pomeni obdelavo osebnih podatkov. Ker obdelava osebnih podatkov oziroma prisluškovanje ni bila urejena v zakonu, takšno pravno stanje pomeni kršitev 8. čl.

Evropske konvencije o človekovih pravicah (EKČP). Iz tega sledi, da bi morali biti osebni podatki v vsakem primeru konkretizirani v takšni meri, da se ne bi mogel pojaviti noben dvom v obseg posega v informacijsko zasebnost, kar vključuje tudi zahtevo, da mora biti v zakonu določen tudi namen obdelave in nabor podatkov. Zaradi izjemno široke definicije osebnih podatkov, ki so vse, kar se nanaša na posameznika, obdelava osebnih podatkov brez izrecno našteje vrste osebnih podatkov, torej zgolj z generalno klavzulo, pomeni diskrecijo upravljavca zbirke osebnih podatkov in možnost zlorab (prisilitve posameznikov po posredovanju (pre)velikega števila osebnih podatkov) se pri določanju nabora podatkov tako lahko poveča. Podobno kot EKČP je tudi Ustavno sodišče v odločbi OdlUS X, 76, U-I-18/98, Ur. l. RS, št. 37/2001, presojo začelo pri vprašanju, ali je **v zakonih** točno opredeljeno, kateri osebni podatki se smejo zbirati in obdelovati. Ker v konkretnem primeru ni bilo zakonskih določb, v katerih bi bili osebni podatki opredeljeni, je bil izpodbijani predpis v neskladju z 2. odst. 38. člena Ustave.

V še eni odločbi, odločbi št. U-I-174/94 je Ustavno sodišče zapisalo, da RTV Slovenija nima zakonske podlage za to, da bi od naročnikov zahtevala prijavo določenih osebnih podatkov in da bi vodila evidenco teh podatkov, zato so določbe pravilnika, ki to urejajo, v nasprotju z drugim odstavkom 38. člena Ustave, po katerem zbiranje, obdelovanje in namen uporabe osebnih podatkov določa zakon. Na tej podlagi je Ustavno sodišče v Pravilniku o načinu prijavljanja in odjavljanja televizijskih in radijskih sprejemnikov, o evidenci naročnikov ter o načinu plačevanja RTV-naročnine razveljavilo: 4., 5., 6., 7. in 8. člen ter drugi odstavek 21. člena.

Podobno pa je Ustavno sodišče zapisalo tudi v odločbi št. U-I-18/98, ko je razveljavilo drugi odstavek 34. člena Zakona o davčnem postopku (v nadaljevanju ZDavP), ker izpodbijana zakonska določba, ob tem, ko pristojnega ministra pooblašča, da predpiše vsebino osebnih podatkov, določno ni opredelila, kateri osebni podatki so to. Razveljavljena določba drugega odstavka 34. člena ZDavP je namreč določala, da morajo pravne in druge osebe, zasebniki, državni in drugi organi ter organi lokalnih skupnosti dostaviti davčnemu organu (davčna uprava) do 31. januarja tekočega leta podatke za odmero dohodnine za preteklo leto, ki vsebujejo tudi davčno številko zavezanca. Izpisek teh podatkov morajo dostaviti tudi zavezancem za dohodnino. Vsebino podatkov, obliko in način dostave podatkov predpiše minister, pristojen za finance. Ustavno sodišče je zapisalo, da vsako zbiranje in obdelovanje osebnih podatkov predstavlja poseg v ustavno pravico do varstva osebnih podatkov, poseg pa je dopusten le, če je v zakonu določno opredeljeno, kateri podatki se smejo zbirati in obdelovati, za kakšen namen jih je dovoljeno uporabiti, nadzor nad zbiranjem, obdelovanjem in uporabo ter varstvo tajnosti zbranih osebnih podatkov. Namen zbiranja osebnih podatkov mora biti ustavno dopusten, zbirati pa se smejo le osebni podatki, ki so primerni in nujno potrebni za uresničitev zakonsko opredeljenega namena. To pomeni, da mora presoja, skladno z načelom sorazmernosti, opraviti že zakonodajalec in presoditi, **kateri** osebni podatki so potrebni in primerni za doseg namena, ki ga določa zakon. V tem primeru pa izpodbijani zakon ne določa niti namena niti nabora osebnih podatkov.

Iz ustaljene sodne prakse Ustavnega sodišča torej nedvoumno izhaja, da je pravno področje varstva osebnih podatkov treba urejati **(samo) z zakonom** in to na način, ki ne dopušča dvoma v določnost osebnih podatkov. Zakonska norma mora zadostiti tudi zahtevi po **lex**

certa. V njej ne sme biti nejasnosti dvoumnosti ali pomensko ohlapnih besed, saj se v nasprotnem primeru na stežaj odpirajo vrata samovolji in arbitrarni uporabi zakona, ki je pri posegih v temeljne človekove pravice najstrožje prepovedana. Predvsem se morajo določno in natančno urediti vsakršni posegi v človekove pravice.

ZBan-1 v izpodbijani določbi določa zgolj obdelavo osebnih podatkov, vendar ne določa, kateri so ti osebni podatki. To pomeni, da je nabor podatkov prepuščen vsakokratni arbitrarni presoji Združenja bank Slovenije (v nadaljevanju ZBS) in članic združenja, katere osebne podatke bodo ti bančni subjekti zahtevali in obdelovali. Veljavna zakonska ureditev namreč ne določa vrste – nabora osebnih podatkov. Po določbi 3. odstavka 390. člena morajo namreč vse banke, ne glede na to, ali so članice bančnega interesnega združenja ali ne, organizirati sistem izmenjave informacij o boniteti strank, ki so fizične osebe, med bankami iz 4. točke drugega odstavka 215. člena tega zakona. Takšno urejanje pa je v nasprotju z ustavo.

Po določbi 3. odstavka 390. člena ZBan-1, lahko ta sistem za banke organizira tudi bančno interesno združenje. Po določbi 4. odstavka istega člena, morajo banke v sistem iz tretjega odstavka tega člena posredovati informacije o boniteti svojih strank. Ker v zakonu vrsta osebnih podatkov ni določena, je bila ta materija urejena v obliki Dogovora o postavitvi in uporabi informacijskega sistema SISBON (v nadaljevanju Dogovor), ki so ga sklenili ZBS, banke in hranilnice, ki so članice tega združenja, in družba SRS.SI kot pogodbeni obdelovalec. Dogovor po določbi 10. točke začne veljati, ko k njemu pristopijo vse članice. Med sicer predvidenimi podpisniki zaenkrat še ni drugih ustanov pristopnic, to je tistih ustanov, ki niso banke in hranilnice (v nadaljevanju pristopnice). Za slednje je predvideno, da k Dogovoru pristopijo s podpisom posebne pogodbe. Iz 5. odstavka 3. točke Dogovora izhaja, da se članice in pristopnice zavezujejo, da bodo v sistem SISBON vnašale tiste osebne podatke svojih komitentov, ki so določene v prilogi št. 2 k temu Dogovoru – SISBON Specifikacija. Po cit. določbi se bodo v sistem SISBON vnašali matični podatki o komitentu, matični podatki o poslih in poslovni dogodki, ki vplivajo na potek posla ter poslovni dogodki, ki niso v skladu s pogodbo. Vsi podatki se nanašajo na komitenta.

Kot matični podatki o komitentu se v sistem SISBON vnašajo in obdelujejo naslednji podatki:

- davčna številka,
- osebno ime,
- datum in kraj rojstva,
- naslov stalnega prebivališča,
- naslov začasnega prebivališča,
- zaposlitev.

Čas hranjenja teh podatkov je, dokler se v SISBONU nahaja podatek o kateremkoli poslu pri katerikoli podpisnici dogovora.

Kot matični podatki o poslu se v sistem SISBON vnašajo naslednji podatki:

- vrsta posla (osebni računi, izredni limit, posojila, kreditne kartice, poroštva drugih),
- datum sklenitve posla,

- oznaka valute,
- znesek ob odobritvi,
- znesek anuitete oziroma obroka,
- vrsta anuitete oziroma obroka,
- odplačilna doba v mesecih,
- podatki o moratoriju,
- datum vnosa.

Čas hranjenja teh podatkov je 6 let po zapadlosti ali ukinitvi posla.

Kot poslovni dogodki, ki vplivajo na potek posla, se v SISBON vnašajo naslednji podatki:

- odplačilo dolga,
- predčasno poplačilo,
- sprememba odplačilne dobe,
- sprememba obroka.

Čas hranjenja teh podatkov je 6 let po zapadlosti posla ali datumu dogodka.

Kot poslovni dogodki, ki niso v skladu s pogodbo, se v SISBON vnašajo naslednji podatki:

- odpoved posla zaradi neplačila dolga,
- neplačan zapadli dolg,
- blokiranje,
- deblokiranje.

Čas hranjenja teh podatkov je 6 let po datumu dogodka.

Banke so zgoraj navedene osebne podatke pričele vnašati v sistem SISBON 1.1.2008. Po definiciji iz Dogovora (točka 1.2.) pomeni sistem SISBON slovenski informacijski sistem bonitet, ki je elektronski in omogoča avtomatsko obdelavo osebnih podatkov, to je: zbiranje, shranjevanje, združevanje, spreminjanje, uporabo ali sporočanje, vključno s prenosom, iskanjem, blokiranjem in brisanjem osebnih podatkov komitentov, članic in pristopnic k temu dogovoru, skladno z določili o poteku rokov hrambe podatkov. Kot komitent se po isti določbi šteje posameznik kot fizična oseba, ki ima pri članici ali pristopnici ali pri več njih vzpostavljeno pogodbeno obveznost iz poslov, navedenih v specifikaciji SISBON, ali namerava vzpostaviti tovrstno obveznost kot potencialni dolžnik nasproti kateri od članic ali pristopnic in je v ta namen podpisal pisno privolitev, oziroma je obdelava osebnih podatkov določena z zakonom. Po isti določbi se kot komitenti upoštevajo tudi posamezniki kot fizične osebe, ki sklepajo druge posle z dejanskim ali potencialnim kreditnim rizikom s članicami ali pristopnicami. Članice in pristopnice so določene kot upravljavke osebnih podatkov, ki obdelujejo osebne podatke svojih komitentov, obenem pa so tudi uporabnice osebnih podatkov posameznih komitentov. Upravljavke – članice (banke in hranilnice) obdelujejo osebne podatke v sistemu SISBON na podlagi zakona (215. in 390. člen ZBan1), upravljavke – pristopnice pa na podlagi komitentove pisne osebne privolitve. To izhaja iz 1.2. točke Dogovora (definicije), ki določa, da je zakonska podlaga za vzpostavitev sistema SISBON določena v 215. in 390. člen ZBan-1 ter da na tej podlagi banke in hranilnice obdelujejo, posredujejo in pridobivajo osebne podatke komitentov brez njihove osebne

privolitve. Pisna privolitev komitenta je izjava v pisni obliki, s katero le ta pooblašča pristopnice – ne kreditne ustanove za obdelavo komitentovih osebnih podatkov, ki vključuje tudi posredovanje osebnih podatkov v SISBON in vpogled v njegove osebne podatke. Ker pri bankah in hranilnicah komitent nima možnosti vpliva na nabor osebnih podatkov, niti nima glede določitve nabora osebnih podatkov možnosti izbire med posameznimi bankami in hranilnicami, saj so vse vključene v sistem SISBON, je naloga zakonodajalca, da skrbno (ob spoštovanju načela sorazmernosti) določi nabor osebnih podatkov, še močneje izražena. Osebna privolitev pa niti ni možna, saj Dogovor taksativno našteva nabor podatkov, ki v sistemu SISBON morajo biti, in to brez dvoma izključuje možnost privolitve, saj posameznika postavlja v pozicijo »vzemi ali pusti«, torej v prisilitev. Življenja brez nekega odnosa z vsaj eno od bančnih institucij si re moremo več predstavljati in odklonitev privolitve pomeni izključitev poslovanja z vsemi bančnimi institucijami v Sloveniji. Ne bo odveč omeniti, da sam Dogovor pod pretvezo privolitve želi širiti uporabo sistema SISBON tudi na finančne institucije, ki jih ZBan ne zajema, kar je tudi v nasprotju z načelom zakonitosti. Povsem jasno namreč je, da SISBON lahko uporabljajo le finančne institucije, za katere veljajo določila tega zakona. Ker obveznost vzpostavitve sistema izmenjave informacij o boniteti strank določa zakon, mora zakon določiti tudi nabor osebnih podatkov in namen obdelave. V takšnih primerih možnost obdelave osebnih podatkov na podlagi osebne privolitve, kar dopušča Zakon o varstvu osebnih podatkov, (praviloma) ni možna.

Obstoječa nedoločnost in nepopolnost zakonske podlage za obdelavo osebnih podatkov, kljub v zakonu določenem namenu (3. odstavek 390. člena ZBan-1 določa sistem izmenjave informacij o boniteti strank, ki so fizične osebe) lahko vodi tudi do različnih interpretacij in s tem nujno do nesorazmerne obdelave osebnih podatkov. Ker ZBan-1 ne določa nabora osebnih podatkov, ki se bodo obdelovali v okviru sistema SISBON, je določanje nabora tako prepuščeno vsakokratni vsebini Dogovora med bankami in hranilnicami. Iz 10. točke Dogovora je celo razvidno, da lahko spremembe Dogovora predlaga vsaka podpisnica in nadzorni svet ZBS, spremembe pa stopijo v veljavo, ko se z njimi strinja dve tretjini članic, merjeno z višino članarine. To pomeni tudi, da se bo nabor osebnih podatkov, ki se bodo obdelovali v sistemu SISBON, v prihodnje lahko spreminjal med drugim tudi zaradi sprememb bančne ponudbe, ki se nanaša na zadolževanje, razvoj novih poslov oziroma nadgradenj sistema in zaradi vključevanja v evropske sisteme kreditnih birojev. Ker je pglavitni namen sistema SISBON sprejem odločitve banke oziroma hranilnice o kreditni sposobnosti posameznega komitenta in s tem dostopnost ali nedostopnost do konkretne bančne storitve (dostop do kreditov, plačilnih in kreditnih kartic itd.), ne more biti določanje nabora osebnih podatkov komitentov, prepuščeno arbitrarnemu dogovoru bank in hranilnic, pač pa je to po določbi 38. člena Ustave RS lahko zaupano samo zakonu. Le zakonodajalec lahko na podlagi načela sorazmernosti in ugotavljanja javnega interesa presodi, kateri podatki so primerni za obdelavo in tako definira dopusten poseg v informacijsko zasebnost posameznikov. Nedoločnost oziroma ne-konkretizacija osebnih podatkov je v 390. členu ZBan-1 očitna. Zakon je namreč bankam in hranilnicam naložil dolžnost izmenjave osebnih podatkov, ni pa obenem določil tudi, katere vrste osebnih podatkov se bodo lahko zbirale in obdelovale v okviru sistema za izmenjavo podatkov (SISBON). To pomeni, da je zakon podelil pravico in dolžnost arbitrarnega določanja nabora osebnih podatkov samim bankam in hranilnicam. Le ZBan-1 ali drug področni zakon lahko določa nabor osebnih podatkov, pri

določanju nabora pa bo zakonodajalec, kot že rečeno, moral slediti načelu sorazmernosti. Ustava namreč v 15. členu določa, da so človekove pravice in temeljne svoboščine omejene samo s pravicami drugih in v primerih, ki jih določa ustava. Vsaka omejitev pa pomeni izjemo in mora biti v zakonu čim bolj natančno in določno urejena.

Državi je prepovedan vsak poseg v pravice in svoboščine posameznika, razen tistih, ki so izrecno dovoljeni. 38. člen Ustave zagotavlja varstvo osebnih podatkov in določa, da je prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. V drugem odstavku 38. člena Ustave pa je določeno, da mora zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnost osebnih podatkov določati zakon. Temeljna vrednota Ustave, iz katere je treba izhajati, je varstvo posameznika pred posegi države.

V vsakem primeru trka dveh ali več ustavnih pravic je torej treba spoštovati načelo praktične konkordance oziroma sorazmernosti, tako da je določeno področje varovanja dopustno omejiti samo, kadar to terjajo pravice drugih in v primerih, ki jih določa ustava (tretji odstavek 15. člena). Obseg varovanja vsake pravice se zato lahko zmanjša le v tistem obsegu, ki je nujno potreben za uveljavljanje druge pravice. To pomeni, da so omejitve in posegi v človekove pravice v določenih primerih ustavno dopustni, in sicer takrat, kadar to zahtevajo pravice drugih in v primerih, ki jih določa ustava. Dopustnost omejitev oziroma posegov v človekove pravice se presoja s testom sorazmernosti, ki izhaja iz 2. člena Ustave, ki določa, da je Republika Slovenija pravna država. Iz načela pravne države izhaja tudi, da mora zakonodajalec določno in nedvoumno urediti pooblastilo organa, ki posega v človekove pravice in temeljne svoboščine.

Prepoved čezmernih posegov države oziroma načelo sorazmernosti je prav z odločitvami Ustavnega sodišča dobilo ustavni rang splošnega ustavnega načela, ki zavezuje vse državne organe, torej tudi zakonodajalca. Človekove pravice namreč zakonodajalca vežejo tudi v vseh tistih primerih, kjer mu sicer Ustava izrecno dopušča možnost zakonskega urejanja in s tem tudi omejevanja posameznih ustavno varovanih pravic in svoboščin. Poleg zahteve, da so takšne omejitve dopustne samo z zakonom in da morajo biti že v samem zakonu podani bistveni kriteriji (jasna določitev vsebine, namena in obsega urejanja) za nadaljnje delovanje, mora biti v samem zakonu spoštovano tudi načelo sorazmernosti. S to zahtevo, ki izvira iz načela pravne države, se postavlja omejitev zakonodajalčevim omejitvam človekovih pravic in temeljnih svoboščin in vzpostavlja kvalificirana povezava med zakonodajalčevim motivom in namenom, ki ga zasleduje, ter sredstvi in pravno normativnimi rešitvami, ki jih v tam namen uporabi (več Komentar Ustave RS, urednik Lovro Šturm, Fakulteta za podiplomske državne in evropske študije, Ljubljana, 2002).

Vsak poseg, to je obseg prizadetosti varovane dobrine, mora biti v sorazmerju z vrednostjo zastavljenih zakonodajnih ciljev. Tež legitimnih posegov zakonodajalca je potrebno zmanjšati do mere, ki še zagotavlja doseganje postavljenih ciljev in tako vzpostaviti razumno ravnovesje med vrednostjo teh ciljev in težo posegov. Prav tako je v nasprotju z ustavo konkretiziranje osebnih podatkov v aktu, hierarhično nižjem od zakona. Osebni podatki morajo na podlagi 38. čl. Ustave RS biti določno opredeljeni že v zakonu. Zakonska dikcija o "izmenjavi informacij o boniteti strank" ne ustreza takšni stopnji dobčnosti, kot jo zahteva določba 38. čl. Ustave RS, saj omogoča preveliko pooblastilo oz. diskrecijo za urejanje

osebnih podatkov v podzakonskem predpisu, še več, zgolj v dogovoru med samimi upravljavci osebnih podatkov. Prepuščanje urejanja kakršnekoli obdelave osebnih podatkov, ki vključuje tudi posredovanje osebnih podatkov, podzakonskemu predpisu ali celo medsebojnemu dogovoru članic združenja bank, ni skladna z zahtevo po strogi vezanosti na zakon pri obdelavi osebnih podatkov na podlagi 38. čl. Ustave RS. Iz tega razloga ni mogoče pristati na podrobnejšo ureditev varstva osebnih podatkov v podzakonskem predpisu oziroma dogovoru članic konkretnega združenja, ampak bi bilo treba vrsto posredovanih osebnih podatkov v celoti določiti v zakonu.

Izpodbijane določbe so po oceni vlagatelja zahteve v neskladju z 38. čl. Ustave, zato Informacijski pooblaščenec

p r e d l a g a:

da Ustavno sodišče RS oceni ustavnost in zakonitost vseh izpodbijanih določb ZBan-1, ugotovi njihovo neskladnost z Ustavo ter jih razveljavi.

Informacijski pooblaščenec
Nataša Pirc Musar, univ. dipl. prav.,
Pooblaščenka

Vročiti:

- naslovníku,
- zbirka dokumentarnega gradiva, tu.