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: 0612-190/2010/
Datum: 1. 3. 2011

Informacijski pooblaščenec izdaja po državnem nadzorniku za varstvo osebnih podatkov na podlagi 2. in 8. člena Zakona o Informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A, v nadaljevanju ZInfP), 54. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07-UPB1, v nadaljevanju ZVOP-1) ter drugega odstavka 28. člena, petega odstavka 29. člena in 32. člena Zakona o inšpekcijskem nadzoru (Uradni list RS, št. 43/07 - UPB1, v nadaljevanju ZIN) v zadevi inšpekcijskega nadzora nad izvajanjem določb ZVOP-1 zoper zavezanca ……., po uradni dolžnosti naslednjo

O D L O Č B O

I. Zavezanec …… mora **v roku 60 dni** od dneva vročitve te odločbe pri elektronskem naročanju na spletni strani zavezanca zavarovati prenos osebnih podatkov z uporabo uveljavljenih kriptografskih metod, ki varujejo zaupnost in celovitost posredovanih podatkov.

II. Zavezanec mora o izvršenem ukrepu iz I. točke izreka te odločbe v roku 5 dni po izvršitvi pisno obvestiti Informacijskega pooblaščenca.

III. V tem postopku posebni stroški niso nastali.

O b r a z l o ž i t e v

I. Postopek inšpekcijskega nadzora in ugotovitve

Državni nadzornik za varstvo osebnih podatkov pri Informacijskem pooblaščencu (v nadaljevanju nadzornik) je prejel prijavo, ki se je nanašala na sum neustreznega zavarovanja osebnih podatkov pri uporabi elektronskega naročanja, ki je možno na spletni strani zavezanca na naslovu http://www..... Z namenom ugotovitve dejanskega stanja je nadzornik dne 12. 1. 2011 zavezanca pozval k podaji pisnega pojasnila in izjave, iz katere bo razvidno, katere osebe imajo dostop do podatkov, ki jih posameznik sporoči bolnišnici prek spletne strani http://www...., kje in kako dolgo se podatki, prejeti preko omenjene strani hranijo in kdaj se brišejo, kako je urejena pogodbena obdelava osebnih podatkov z zunanjim izvajalcem podjetjem …… d.o.o.

Zavezanec je na poziv nadzornika pravočasno poslal pisni odgovor, v katerem je podal pojasnila na vse točke poziva. Nadzornik je ob pregledu odgovora zavezanca in priloženih pravilnikov o varstvu osebnih podatkov zavezanca in pogodbenega obdelovalca, ki zavezancu nudi storitve vzdrževanja spletne strani, ugotovil, da pri ureditvi pogodbene obdelave ni bilo storjenih kršitev. Zavezanec je skladno z določili 11. člena ZVOP-1 pogodbeno obdelavo uredil s pisno pogodbo, v kateri so s sklicem na omenjena pravilnika o zavarovanju osebnih podatkov ustrezno urejeni tudi ukrepi in postopki za zavarovanje osebnih podatkov, kot to določa 24. člen ZVOP-1.

Glede zavarovanja osebnih podatkov, ki jih zavezanec pri elektronskem naročanju prejme preko svoje spletne strani, je zavezanec pojasnil, da imata dostop do teh podatkov samo 2 osebi pri zavezancu in da je dostop zavarovan z uporabniškim imenom in geslom. Po oddaji naročila na spletni strani se kreira elektronsko sporočilo, ki se hrani v predalu e-pošte in se v obliki natisnjene e-pošte vodi v ustreznem fasciklu s potrebnimi zaznamki. To dokumentacijo zaposlena redno pregledujete in v roku 6-mesecev po izvedeni storitve oziroma izbrisu podatkov dokument uničita in izbrišeta elektronsko pošto. 3. odstavek 15. člena Zakona o pacientovih pravicah (Ur. l. RS št. 15/2008; ZPacP) namreč določa, da se podatki v čakalnem seznamu in podatki o morebitnem spreminjanju vrstnega reda skupaj z obrazložitvijo okoliščin, ki narekujejo spreminjanje vrstnega reda, hranijo šest mesecev po opravljeni zdravstveni storitvi oziroma izbrisu podatkov.

Državni nadzornik je ugotovil, da spletna stran zavezanca za elektronsko naročanje (http://www.....) ne uporablja uveljavljenih kriptografskih metod za zagotovitev zaupnosti in celovitosti podatkov, ki se posredujejo pri uporabi tovrstnega naročanja. Spletna stran se uporabniku ne izkazuje z zaupanja vrednim certifikatom, sam prenos podatkov med brskalnikom pri uporabniku in internetnim stražnikom zavezanca pa ni zavarovan s kriptografskimi metodami, ki preprečujejo prisluškovanje ali spreminjanje podatkov, ki se prenašajo.

II. Navedba določb predpisov, na katere se opira odločba

Osebni podatek je po določbi 1. točke 6. člena ZVOP-1 katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, ob tem da je posameznik v skladu 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.

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 del zbirke osebnih podatkov ali so 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.

Upravljavec osebnih podatkov je v 6. točki 6. člena ZVOP-1 definiran kot fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.

Občutljivi osebni podatki so po določbi 19. točke 6. člena ZVOP-1 opredeljeni kot podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške (v nadaljnjem besedilu: prekrškovne evidence); občutljivi osebni podatki so tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.

2. odstavek 14. člena ZVOP-1 določa, da se pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

III. Razlogi, ki glede na ugotovljeno dejansko stanje narekujejo takšno odločbo

Kot je razvidno iz zgoraj navedenih ugotovitev zavezanec legitimno zasleduje cilj uporabe različnih komunikacijskih kanalov za naročanje na zdravstvene storitve in pacientom omogoča naročanje tudi preko spletne strani zavezanca, kar dopušča tudi 2. odstavek 10. člena Pravilnika o najdaljših dopustnih čakalnih dobah za posamezne zdravstvene storitve in o načinu vodenja čakalnih seznamov. Po pojasnilu zavezanca so podatki, ki jih pacient vnese na spletni strani enaki kot podatki, ki bi jih moral sporočiti pri telefonskem naročanju ali pri naročanju po pošti.

Državni nadzornik glede obsega zahtevanih podatkov ob upoštevanju načela sorazmernosti ni ugotovil nepravilnosti, a je ugotovil, da zavarovanje osebnih podatkov pri elektronskem naročanju med prenosom ni skladno z zahtevami ZVOP-1. Pacient namreč zavezancu prek njegove spletne strani poleg svojih kontaktnih in identifikacijskih podatkov sporoči tudi podatke o enoličnih identifikatorjih (EMŠO in številka zdravstvenega zavarovanja) ter neobvezno tudi podatke o ambulanti, zdravniku in opisu težav. Glede na opredelitev občutljivih osebnih podatkov iz 19. točke 6. člena ZVOP-1 moramo podatke o ambulanti, zdravniku in opisu težav šteti za

občutljive osebne podatke, s tem pa mora zavezanec skladno z določbo 3. odstavka 24. člena ZVOP-1 poskrbeti za postopke in ukrepe zavarovanja osebnih podatkov, ki so skladni z naravo in tveganjem, ki jih obdelava takšnih podatkov prinaša.

Zavarovanje občutljivih osebnih podatkov natančneje opredeljuje tudi 2. odstavek 14. člena ZVOP-1, ki določa, da se pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

Državni nadzornik ugotavlja, da je zahtevi iz 2. odstavka 14. člena ZVOP-1 v konkretni situaciji smiselno, možno in potrebno zadostiti z uporabo **uveljavljenih kriptografskih metod, ki varujejo zaupnost in celovitost sporočil**, ki se posredujejo določeni spletni strani. Gre za metode, ki aplikacijam strežnik/klient omogočajo varno komunikacijo, ki preprečuje prisluškovanje in manipulacijo s posredovanimi podatki, zagotovi pa se z uporabo zaupanja vrednih **digitalnih strežniških potrdil** in uporabe mednarodno uveljavljenih protokolov, kot so npr. **TLS/SSL** (Transport Layer Security/ Secure Sockets Layer). Uvedba tovrstnih metod lahko poleg večje varnosti omogoči tudi dvig zaupanja pri uporabnikih spletne strani. Spletna stran, ki uporablja takšne metode se namreč uporabniku izkazuje z digitalnim potrdilom, kar se z uporabniškega vidika odrazi kot predpona **https** (namesto http), sodobni brskalniki pa uporabniku spletnega brskalnika takšne varnostne ukrepe tudi grafično ponazorijo in s tem uporabniku zagotovijo, da je povezava na to spletno stran varna in da nepooblaščene tretje osebe ne morejo prestreči ali spremeniti vsebino prenesenih podatkov.

Glede na to, da se pri uporabi elektronskega naročanja v praksi ni mogoče izogniti posredovanju občutljivih osebnih podatkov, je za njihovo varnost med prenosom treba poskrbeti z ustreznimi in sorazmernimi ukrepi. Nadzornik je zato zavezancu odredil, da mora v roku 60 dni od vročitve te odločbe za zagotovitev ustreznega zavarovanja občutljivih osebnih podatkov pri sistemu elektronskega naročanja uvesti uporabo kriptografskih metod, ki varujejo zaupnost in celovitost sporočil, ki se posredujejo spletni strani zavezanca za elektronsko naročanje.

IV. Sklepno

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). Glede na obrazloženo je bilo potrebno zavezancu na podlagi 1. točke prvega odstavka 54. člena ZVOP-1 odrediti sprejem ukrepa za zavarovanje občutljivih osebnih podatkov, ki se prenašajo preko telekomunikacijskih omrežij in na ta način zagotoviti skladnost z določbo 2. odstavka 14. člena ZVOP-1.

Izrek, da je zavezanec o izvršitvi ukrepov iz I. točke izreka te odločbe dolžan v roku 5 dni po izvršitvi pisno obvestiti Informacijskega pooblaščenca, temelji na določbi petega odstavka 29. člena ZIN, kjer je določeno, da če inšpektor odredi odpravo nepravilnosti in pomanjkljivosti ter zavezancu določi rok za njihovo odpravo, mora zavezanec o odpravljenih nepravilnostih takoj obvestiti inšpektorja.

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 vloži pri pristojnem sodišču neposredno pisno ali se mu pošlje po pošti. Tožbi v dveh izvodih je treba priložiti to odločbo v izvirniku ali neoverjeno kopijo.

mag. Andrej TOMŠIČ,
državni nadzornik
za varstvo osebnih podatkov,
namestnik informacijske pooblaščenke

Vročiti:

1. ……, z vročilnico po ZUP;
2. arhiv, tu.