REPUBLIKA SLOVENIJA
INFORMACIJSKI POOBLAŠČENEC
Zaloška 59, 1000 Ljubljana, Slovenija
T: 01 230 9730
F: 01 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Številka: 0612-181/2016/6
Datum: 26. 9. 2016

Informacijski pooblaščenec Republike Slovenije (v nadaljevanju IP) izdaja po državnem nadzorniku za varstvo osebnih podatkov [redacted] (v nadaljevanju državni nadzornik), na podlagi četrtega odstavka 135. člena Zakona o splošnem upravnem postopku (Uradni list RS, št. 24/06-UPB2 s spremembami in dopolnitvami; v nadaljevanju ZUP) v zvezi s 50. členom Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07-UPB1; v nadaljevanju ZVOP-1), drugim odstavkom 3. člena Zakona o inšpekcijskem nadzoru (Uradni list RS, št. 43/07-UPB1 in 40/14, v nadaljevanju ZIN) ter 2. in 8. členom Zakona o informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A; v nadaljevanju ZInfP), v zadevi opravljanja inšpekcijskega nadzora nad izvajanjem določb Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07, uradno prečiščeno besedilo, v nadaljevanju ZVOP-1) pri zavezancu Univerzitetni klinični center Ljubljana, Zaloška cesta 2, 1000 Ljubljana (v nadaljevanju zavezanec), po uradni dolžnosti naslednji

SKLEP:

1. Postopek inšpekcijskega nadzora, ki ga Pooblaščenec zoper zavezanca vodi pod številko 0612-181/2016, se ustavi.
2. Stroški v postopku niso nastali.

OBRAZLOŽITEV:

IP je prejel prijavo v kateri je bilo navedeno, da naj zavezanec ne bi ustrezno zavaroval osebnih in občutljivih osebnih podatkov na spletni strani http://napotnica.kclj.si/. Iz prijave je izhajalo, da naj bi zgolj vnos url povezave http://napotnica.kclj.si/UKCBookingReservation/ v spletni brskalnik omogočil dostop do občutljivih osebnih podatkov, med drugim tudi diagnoz posameznih pacientov. Dne 9.9.2016 je IP opravil ogled spletne strani zavezanca in o ugotovitvah sestavil zapisnik št. 0612-181/2016/2. Iz zapisnika, ki ga je IP 12.9.2016 skupaj s pozivom poslal zavezancu, je razvidno, da je dne 9.9.2016 vnos url povezave http://napotnica.kclj.si/UKCBookingReservation/document/document_list.xhtml v spletni brskalnik omogočil nezaščiten dostop do večjega številka zdravstvene in druge dokumentacije, vključno z napotnicami, ki so vsebovale osebne in občutljive osebne podatke. Vnos povezave http://napotnica.kclj.si/UKCBookingReservation/person/person_list.xhtml pa je omogočil nezaščiten dostop do osebnih podatkov večjega števila zaposlenih pri zavezancu.

Zavezanec je 9.9.2016 (isti dan, ko je bil s strani IP obveščen o varnostnem incidentu) po elektronski pošti poslal poročilo o razlogih zaradi katerih je do incidenta prišlo ter o ukrepih, ki jih je izvedel, da je varnostno luknjo odpravil. Prav tako je dne 20.9.2016 posredoval na IP še pisno pojasnilo, v katerem je dodatno pojasnil, da je bil dostop do omenjenih osebnih in občutljivih osebnih podatkov posledica varnostne luknje, ki jo je odkril anonimni napadalec, ki je nato obvestil IP. Zavezanec poudarja, da javnost ni poznala spornega url naslova, ki je omogočal dostop do podatkov, pač pa zgolj napadalec, ki je bil zelo verjetno dobro podučen o informacijskem sistemu v okviru katerega so se osebni podatki obdelovali. Iz dnevniškega zapisa, ki ga je zavezanec kot prilogo poslal skupaj s pojasnilom, je

razvidno, da je poleg IP, ki je do spletne strani dostopal dne 9.9.2016 z namenom preverjanja navedb iz prijave, do podatkov dostopal zgolj napadalec in sicer……..……..

V pisnem pojasnilu zavezanec navaja, da so vzpostavili intervencijsko skupino strokovnjakov in izvedli zaporedje varnostnih ukrepov:

- omejili pravice uporabnikov, ki uporabljajo aplikacijo Napotnica;
- odvzeli pravico za branje in pisanje dokumentov, ki jih naloži uporabnik aplikacije;
- spremenili aplikativna gesla v aplikacijah, ki so komunicirale z napadeno aplikacijo;
- v testni scenarij dodali zahtevo, da se posebej testira tudi to varnostno luknjo (ki je sicer odpravljena, vendar gre za preventivne preglede);
- druge tehnične ukrepe za zagotavljanje višje stopnje varnosti.

Prav tako je zavezanec po tem, ko ga je IP dne 9.9.2016 seznanil z incidentom, o tem obvestil SI-CERT in sicer dne 9.9.2016 ob 17:10. Pisno obvestilo je zavezanec kot prilogo dodal k pojasnilu, ki ga je poslal IP.

Na podlagi vsega navedenega Pooblaščenec ugotavlja, da je zavezanec ugotovljene nepravilnost odpravil, zato je bilo treba na podlagi 4. odst. 135. člena ZUP, v povezavi z 2. odst. 3. člena ZIN, postopek inšpekcijskega nadzora ustaviti, saj bo IP o ugotovljeni kršitvi določb ZVOP-1 v zvezi z neustreznim zagotavljanjem varnosti pri obdelavi občutljivih osebnih podatkov odločal v postopku za prekrške.

Ta sklep je izdan po uradni dolžnosti in je na podlagi 22. člena Zakona o upravnih taksah (ZUT; Uradni list RS, št. 106/2010-UPB5) takse prost.

Pouk o pravnem sredstvu: Zoper ta sklep po določbah 55. člena ZVOP-1 ni dovoljena pritožba, temveč je dopustno sprožiti upravni spor. Upravni spor se sproži s tožbo, ki se vloži v 30 dneh od vročitve sklepa na Upravno sodišče Republike Slovenije, Fajfarjeva 33, 1000 Ljubljana. Tožba se lahko pošlje po pošti, vloži pisno ali da ustno na zapisnik pri sodišču. Tožba z morebitnimi prilogami se vloži najmanj v treh izvodih. Tožbi je treba priložiti tudi ta sklep v izvirniku ali prepisu.

Informacijski pooblaščenec

[redacted]

državni nadzornik

za varstvo osebnih podatkov