EISEP – SKLADNI ZAJTRK

4. marca 2026 je v kavarni Slamič potekal prvi EISEP skladni zajtrk letošnjega leta. Tokratni gost je bil mag. Andrej Tomšič, namestnik informacijske pooblaščenke, ki se ukvarja s pravno-tehnološkimi in družbenimi izzivi zasebnosti, o čemer je tudi tekel pogovor.

Uvodoma je pojasnil, kaj je pravica do zasebnosti ter kaj to zares pomeni. Ne gre namreč za to, da posameznik ničesar ne skriva, temveč to pomeni le, da mu pripada pravica, da določene zasebne informacije ne postanejo javne.

Pravica do zasebnosti nam omogoča, da lahko sami izberemo, s kom bomo delili katere informacije ter v kakšnem obsegu. V današnjem času menim, da je ustrezen pravni okvir še posebej pomemben zaradi razširjene uporabe socialnih omrežij, kjer lahko uporabniki delijo osebne informacije, le-te pa se zaradi narave platforme lahko hitro razširijo ter postanejo dostopne širšemu krogu ljudi. Brez regulacije in nadzora, bi bili naši osebni podatki prosto dostopni vsakomur, popolnoma brez omejitev, kar bi lahko vodilo v zlorabe, v skrajnejših primerih pa tudi v krajo identitete.

Število vseh zadev, ki jih obravnava Informacijski pooblaščenec kot organ, se skozi leta viša. V letu 2024 je Informacijski pooblaščenec obravnaval 1030 novih zadev, leto prej 1021 ter 971 v letu 2022. V lanskem letu je informacijski pooblaščenec vodil 846 inšpekcijski postopkov in izdal 981 pisnih mnenj. Letno poročilo za leto 2025 sicer še ni javno objavljeno, vendar je mag. Tomšič navedel, da so številke v primerjavi z letom 2024 višje. Nadalje je nadzornik opozoril na pomembnost sistemskih kršitev, ki jih ni smiselno reševati z individualnimi inšpekcijskimi postopki, temveč tako, da informacijski pooblaščenec pošlje poziv subjektu ter poda možne načine za odpravo sistemskih kršitev.

Postopki nadzora ne tečejo le na podlagi prijav, pač pa se jih veliko začne tudi po uradni dolžnosti. Večinoma se v takih primerih naredi oceno tveganja, kar pomeni, da se določijo področja, ki se bodo tisto leto preverjala, nato pa se postopoma preverja subjekte, ki delujejo na tem področju. Na tak način se ustvari pritisk med subjekti, ki nato poskušajo sami odpraviti kršitve in se tako izogniti sankcijam, ki bi jih ob ugotovitvah kršitev naložil informacijski pooblaščenec. Doslej je bilo veliko pozornosti na video-nadzoru, od koder tudi največ ugotovljenih kršitev. Veliko prijav pa je bilo vloženih tudi zaradi suma nezakonitega razkrivanja in posredovanja osebnih podatkov neupravičenim osebam ter zaradi nezakonitega ali prekomernega zbiranja osebnih podatkov.

Mag. Tomšič je v nadaljevanju odgovoril na vprašanje iz publike glede snemanja klicev ter digitalno izvedenih sestankov. Izpostavil je, da soglasja niso vedno popolnoma aktivno podana, zato je bistveno, da so udeleženci obveščeni o tem, da se pogovor ali sestanek snema, ter kaj se bo zgodilo s pridobljenimi podatki. Poleg tega pa je poudaril

potrebo po reformi zakonodaje na tem področju, saj se pravila zakona nanašajo le na telefonske klice, kar v današnjem času zaradi razvoja tehnologije ni najbolj ustrezno.

Nadalje je pogovor tekel o kaznih, ki doletijo kršitelje pravice do zasebnosti ali varstva osebnih podatkov. Pri nas informacijski pooblaščenec izreka precej nižje kazni kot v ostalih državah članicah Evropske unije, kjer znašajo kazni tudi po več milijonov evrov. Leta 2025 je bila ena od najvišje izrečenih kazni pri nas 16.000 € za pravno osebo in 400 € za odgovorno fizično osebo. Glavni kriterij za določitev kazni je upoštevanje stekov. Pri ugotavljanju odgovornosti za prekršek in odmeri kazni nadzornik upošteva zlasti: 1) učinke kršitev na zunanji svet, 2) subjektivni odnos storilca do ravnanja, torej ali je ravnal naklepno ali pa je do posledice prišlo pomotoma, 3) število udeležencev, 4) težo oz. pomen in občutljivost podatkov ter 5) ravnanje storilca pred, med in po dogodku. Veliko vlogo pri odmeri kazni namreč igra skesanje storilca.

Sledil je pogovor o dobrih praksah, kjer je namestnik informacijske pooblaščenke poudaril pomembnost ocene učinkov v zvezi z varstvom osebnih podatkov (t. i. Data Privacy Impact Assessment oz. DPIA), saj lahko le tako podjetja sprejmejo najustreznejše ukrepe. V idealnem primeru bi podjetja izvedla oceno ter to posredovala informacijskemu pooblaščencu, ki bi na podlagi ocene izdal pisno mnenje, ki bi podjetju služilo kot smernica za sprejem ukrepov. Mnenja informacijskega pooblaščenca so namreč nezavezujoča, kar pomeni, da jih subjekti niso dolžni upoštevati. Kljub temu pa služijo kot dobra iztočnica za delovanje podjetja, saj mora informacijski pooblaščenec preveriti formalno popolnost ocene učinka tveganja, ter preučiti, ali je subjekt ustrezno zajel in analiziral morebitna tveganja.

Zadnja tema pogovora je bil Akt o umetni inteligenci, uredba Evropske unije, ki vzpostavlja pravila za uporabo umetne inteligence. Na podlagi uredbe je Slovenija kot ena od prvih držav Evropske unije, sprejela Zakon o izvajanju uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci (ZIUDHPUI), s katerim je podelila pristojnost nadzora petim organom, med katerimi je tudi informacijski pooblaščenec.

Glede Akta o umetni inteligenci, sem mag. Tomšiču postavila vprašanje glede morebitnih neskladnosti med ZVOP-2 in Aktom o umetni inteligenci. Izvedela sem, da sta akta med sabo komplementarna in si zaenkrat ne nasprotujeta. Enako velja tudi za zakon o izvajanju uredbe. Glede same uporabe umetne inteligence je informacijski pooblaščenec najbolj zaskrbljen glede področij, kjer bi umetna inteligenca dejansko lahko sprejemala vsebinske odločitve (npr. glede tega, kdo dobi kredit ali štipendijo), saj je umetna inteligenca lahko pristranska pri svojem odločanju. To zagotovo predstavlja velik problem še posebej, če odločitvi umetne inteligence ne sledi preveritev s človeške strani.

Vprašanja glede zasebnosti, varstva osebnih podatkov ter uporabe umetne inteligence danes zagotovo spadajo med pomembnejša, še posebej zaradi hitrega razvoja

tehnologije in porasta v njeni uporabi. Pogovor z namestnikom informacijske pooblaščenke je tako ponudil koristen vpogled tako v delo organa kot tudi v razvijajočo pravno ureditev na področju umetne inteligence. Slednja je v današnjem času obvezna zaradi naraščajoče priljubljenosti, večinoma med mladimi in otroci. Menim sicer, da umetna inteligenca sama po sebi ni problematična, vendar pa njena uporaba lahko postane tvegana, če ji uporabniki omogočamo dostop do svojih (občutljivejših) osebnih podatkov. Večina se nas namreč ne zaveda, na kakšen se uporabniški podatki zbirajo ter kako in zakaj se obdelujejo. Zato je ključno, da se vzporedno z razvojem tehnologije, razvijajo tudi pravo ter nadzorni mehanizmi, ki omogočajo učinkovito varstvo pravic ter zasebnosti. Pomembno vlogo pri tem pa igrajo tako Evropska unija kot tudi nacionalna zakonodaja ter nadzorni organi.

Lili Preinfalk