REPUBLIKA SLOVENIJA
INFORMACIJSKI POOBLAŠČENEC
Dunajska cesta 22, 1000 Ljubljana
T: 01 230 9730
www.ip-rs.si
gp.ip@ip-rs.si

Številka: 007-15/2026/2
Datum: 14. 5. 2026

Ministrstvo RS za javno upravo
gp.mju@gov.si

Zadeva: Osnutek Pravilnika o izvajanju videokonference v upravnem postopku – MNENJE
Zveza: Vaš dopis št. 007-21/2026/3, prejet dne 22. 4. 2026

Spoštovani,

na podlagi vašega zaprosila, 3. točke prvega odstavka 55. člena Zakona o varstvu osebnih podatkov (ZVOP-2) ter 57. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter razveljavitvi Direktive 95/46/ES (Splošna uredba) v nadaljevanju posredujemo mnenje Informacijskega pooblaščenca (IP) k prejetemu Osnutku Pravilnika o izvajanju videokonference v upravnem postopku (v nadaljevanju: osnutek pravilnika).

Kot je IP opozoril že v svojem mnenju ob spremembah in dopolnitvah Zakona o splošnem upravnem postopku, predstavlja izvedba ustne obravnave prek videokonference vrsto praktičnih in pravnih izzivov, zlasti glede na to, da zakonska ureditev ne zagotavlja ustrezne informacijske infrastrukture za njihovo izvedbo. V praksi to pomeni, da so organi prepuščeni uporabi raznovrstnih informacijskih rešitev, kot so ZOOM, Microsoft Teams, Big Blue Button ipd. Te rešitve lahko predstavljajo pomembna tveganja z vidika varstva osebnih podatkov, zlasti glede urejanja pogodbene obdelave in pogodbenih razmerij s ponudniki storitev, prenosa osebnih podatkov v tretje države, zagotavljanja ustreznih informacij posameznikom o obdelavi njihovih podatkov itd.

IP uvodoma glede na navedeno splošno opozarja, da gre pri izvedbi videokonference načeloma za obdelavo osebnih podatkov, saj je posameznik, ki v upravnem postopku sodeluje preko videokonference, po naravi stvari določen oziroma določljiv. Hkrati gre pri tem lahko tudi za obdelavo osebnih podatkov morebitnih tretjih oseb, ki so naključno prisotne ob posamezniku, predvsem takrat, ko je ločljivost dovolj velika in je posameznik jasno in nedvoumno razviden in bi se bi se ga dalo na ta način identificirati, prepoznati in določiti, ali ko se hkrati s posnetki obdelujejo tudi drugi osebni podatki o posamezniku. Enako velja tudi za izvedbo postopka ugotavljanja istovetnosti z videoidentifikacijo (6. člen). V takih primerih je zato treba zagotoviti spoštovanje vseh obveznosti s področja varstva osebnih podatkov, še posebej pa zagotoviti ustrezno informiranost posameznika v skladu z določbami 13. člena Splošne uredbe (mu torej na predpisan način zagotoviti vse informacije iz tega člena) in poskrbeti za ustrezno varnost osebnih podatkov v skladu z določbami 24. in 32. člena Splošne uredbe.

IP predlaga tudi, da se v 6. členu izrecno zapiše, da se ugotavljanje istovetnosti, ki ga izvede uradna oseba, opravi brez prisotnosti drugih udeležencev oziroma da pri njeni izvedbi ne sme biti vpogled v dokument omogočen tudi drugim udeležencem. To sicer delno že izhaja iz četrtega odstavka 3. člena osnutka pravilnika, vendar zgolj posredno, saj ni izrecno določeno. IP meni, da je s stališča varstva osebnih podatkov ustrezno, da se to jasno in nedvoumno določi v izogib morebitnim dilemam v praksi. V zvezi s 6. členom IP predlaga tudi, da se določi, kako se postopa v primeru, da ugotavljanja istovetnosti z videoidentifikacijo (iz tehničnih ali drugih razlogov) ni mogoče izvesti.

IP v zvezi s 3. členom izpostavlja zlasti drugi odstavek, v zvezi s katerim se najprej sprašuje, kdo opravi oceno stopnje tveganja glede varnosti osebnih podatkov, ob tem pa meni, da tu ne gre upoštevati zgolj

narave upravne zadeve, ampak tudi naravo oziroma vrsto obravnavanih osebnih podatkov v zadevi. Nadalje IP meni, da bo v praksi nekatere v njem predvidene ukrepe (še zlasti v primeru javne videokonference) zelo težko zagotoviti (npr. spreminjanje slike in zvoka, nadzor vklopa in izklopa kamere, …). S tem v zvezi IP izpostavlja tudi določbo četrtega odstavka 4. člena osnutka pravilnika, ki določa, da udeleženec ne sme samovoljno izklapljati slike ali mikrofona. Tukaj se IP sprašuje o dopustnosti tega ukrepa z vidika posega v zasebnost udeleženca in poziva k premisleku, ali ne bi v določenih situacijah veljalo omogočiti možnost izklopa (npr. prihod mladoletnega otroka v kader, napad kašlja ali druge zdravstvene težave, …). IP se sprašuje tudi, kako bo mogoče preprečiti nedovoljeno snemanje z ozirom na to, da vsak udeleženec lahko snema svoj ekran in nasploh na svoji napravi opravlja mnoga različna dejanja (tudi spreminja oziroma megli sliko ipd.).

Glede petega odstavka 3. člena in možnosti deljenje slike zaslona IP meni, da bi veljalo bolj natančno določiti, kdaj ta možnost pride v poštev (npr. kadar je to nujno za izvedbo same obravnave).

IP sklepno izraža pomislek glede tega, ali kateri od trenutnih sistemov v prosti uporabi sploh omogoča izpolnjevanje vseh v osnutku pravilnika predvidenih ukrepov. Ob tem posebej opozarja, da v primerih uporabe precej ponudnikov teh sistemov prihaja tudi do prenosa osebnih podatkov izven EU (zlasti v ZDA), kar pomeni, da je treba zagotoviti tudi spoštovanje določb poglavja V Splošne uredbe v zvezi s prenosom osebnih podatkov v tretje države.

IP sklepno dodaja, da je mnenje omejeno na vidike varstva osebnih podatkov (za katere je pristojen IP), ne pa na druge vidike, ki jih urejata predlog zakona in uredbe.

Hvala za sodelovanje in lep pozdrav,

dr. Jelena Virant Burnik,
Informacijska pooblaščenka

Pripravil:
Matej Sironič,
Svetovalec pooblaščenca I