



Ulica gledališča BTC 2, 1000 Ljubljana

T: 01 478 4778

E: gp.uiv@gov.si

W: <http://www.uiv.gov.si>

X: @URSIV\_Slovenia

Številka: 430-3/2026-1544-2

Datum: 4. 5. 2026

## POVABILO K ODDAJI PONUDBE

za

### EVIDENČNO NAROČILO

»PSIHOLOŠKI DEJAVNIKI RAZUMEVANJA IN UPOŠTEVANJA SPOROČIL  
ORGANOV S PODROČJA INFORMACIJSKE (KIBERNETSKE) VARNOSTI«

NAROČNIK: Urad Vlade RS za informacijsko varnost  
Ulica gledališča BTC 2, 1000 Ljubljana

VRSTA POSTOPKA: Evidenčni postopek

NASLOV NAROČILA: Psihološki dejavniki razumevanja in upoštevanja  
sporočil organov s področja informacijske  
(kibernetske) varnosti

OZNAKA NAROČILA: EVN-430-4/2026

Naročnik vabi vse zainteresirane in usposobljene ponudnike, da sodelujejo v postopku in oddajo ponudbo za predmet tega naročila. Ponudbe morajo biti v celoti pripravljene v skladu s tem povabilom in morajo izpolnjevati vse pogoje za sodelovanje.

### 1. PREDMET NAROČILA

Izvedba raziskovalne študije za potrebe Urada Vlade Republike Slovenije za informacijsko varnost z naslovom **Psihološki dejavniki razumevanja in upoštevanja sporočil organov s področja informacijske (kibernetske) varnosti**, katere namen je ugotoviti, kateri psihološki, vedenjski in komunikacijski dejavniki vplivajo na to, kako podjetja razumejo, interpretirajo in upoštevajo sporočila vladnih organov s področja informacijske oziroma kibernetike varnosti.

Študija mora izhajati iz spoznanja, da na odziv naslovnikov ne vpliva zgolj vsebina sporočila, temveč tudi njegova oblika, način posredovanja, kontekst uporabe ter specifika informacijskih tehnologij in digitalnih komunikacijskih kanalov, prek katerih so sporočila posredovana.

## 1.1 Opis storitev izbranega ponudnika

Ponudnik mora zagotoviti interdisciplinarno izvedbo raziskave. V projektni skupini morata sodelovati najmanj strokovnjak s področja informacijske oziroma kibernetске varnosti in strokovnjak s področja psihologije; zaželeno je tudi izkazano poznavanje vedenjskih intervencij, komuniciranja ali oblikovanja digitalnih vsebin. V kolikor ena oseba pokriva obe področji, je lahko ponudnik tudi posameznik.

Izvajalec mora pred začetkom izvedbe potrditi raziskovalna vprašanja in metodo zbiranja podatkov.

Študija mora vključevati najmanj:

- 1) strukturirani pregled domače in tuje znanstvene ter strokovne literature s področij psihologije, vedenjskih ved, komuniciranja, oblikovanja sporočil, uporabniške izkušnje in informacijske oziroma kibernetске varnosti;
- 2) identifikacijo in razlago ključnih psiholoških dejavnikov, ki vplivajo na zaznavo, razumevanje, zapomljivost, odločanje in vedenjski odziv podjetij ob prejemu varnostnih sporočil državnih organov;
- 3) analizo vpliva vsebinskih in oblikovnih značilnosti sporočil, kot so stavčna struktura, besedni zaklad, dolžina sporočila, vrsta in položaj elementov, vrste pisave, barve, kontrasti, oblike, zvočni in drugi verbalni ter neverbalni elementi;
- 4) pregled ugotovitev o vplivu dejavnikov, povezanih s pozornostjo, kognitivno obremenitvijo, učenjem, normami, konformizmom, odporom, zaupanjem, verodostojnostjo vira in čustvenimi odzivi, vključno z odzivi, kot je strah;
- 5) pripravo analitičnega modela oziroma okvirja dejavnikov, ki vplivajo na učinkovitost sporočil s področja informacijske oziroma kibernetске varnosti;
- 6) empirično preveritev ugotovitev na ustreznem vzorcu podjetij oziroma predstavnikov podjetij, ki so naslovniki tovrstnih sporočil, z uporabo ustrezne kombinacije kvantitativnih in/ali kvalitativnih raziskovalnih metod.

Raziskovalno poročilo mora vsebovati znanstveno utemeljena priporočila za oblikovanje sporočil, ki s svojo vsebino in obliko spodbujajo želene odzive naslovnikov. Priporočila morajo biti pripravljena v obliki konkretnih navodil oziroma smernic za pripravljavce sporočil.

Priporočila morajo posebej naslavljati ukrepe za doseganje večje kognitivne učinkovitosti in odzivnosti, in sicer z vidika:

- vzbujanja in zadrževanja pozornosti na fiziološki in psihološki ravni;
- zaznave in razumevanja pomena verbalnih in neverbalnih informacij;
- zapomljivosti, odločanja in učenja;
- družbenih norm, konformizma in zmanjševanja odpora oziroma ignoriranja vsebine sporočil;
- čustvenih odzivov naslovnikov.

Končni izdelki morajo biti pripravljene v slovenskem jeziku ter predloženi najmanj v PDF in Word obliki; preglednice, izvorni podatki, matrike kodiranja in druge priloge morajo biti

oddani tudi v strojno berljivi obliki (Excel ali CSV), kadar je to glede na naravo gradiva mogoče.

Izvajalec mora zagotoviti metodološki opis zbiranja in obdelave podatkov, sledljivost uporabljenih virov, ponovljivost postopka ter jasno označiti omejitve, predpostavke in morebitne metodološke zadržke raziskave. Zbiranje in obdelava podatkov morata biti skladna z GDPR in drugimi relevantnimi predpisi.

Končni izdelki naj obsegajo najmanj: potrjeno metodologijo, pregled literature, raziskovalne instrumente, analitični okvir dejavnikov, končno poročilo s priporočili, nabor praktičnih smernic oziroma kontrolni seznam za pripravo sporočil ter predstavitev ključnih ugotovitev naročniku.

## **2.1 Terminski plan**

Povabilo k oddaji ponudbe: 4. 5. 2026

Rok za oddajo ponudbe: 23. 5. 2026 do 15.00

Izbor izvajalca: 27. 5. 2026

Izdaja naročilnice: najkasneje 29. 5. 2026

Začetni usklajevalni sestanek in potrditev metodologije: v 15 dneh od uvedbe v delo.

Osnutek končnega poročila: praviloma v petem do sedmem mesecu izvajanja.

Končno poročilo, praktične smernice in predstavitev rezultatov: najpozneje v šestem do devetem mesecu izvajanja.

## **3. POSEBNI POGOJ ZA SODELOVANJE - reference ponudnika**

Prednost imajo ponudniki, ki izkazujejo interdisciplinarno delo na presečišču psihologije in informacijske oziroma kibernetске varnosti ter izkušnje s pripravo uporabnih priporočil, smernic ali vedenjsko utemeljenih komunikacijskih intervencij.

Ponudnik mora izkazati, da v projektni skupini sodelujeta najmanj strokovnjak s področja informacijske oziroma kibernetске varnosti in strokovnjak s področja psihologije. V kolikor ena oseba pokriva obe področji, je lahko ponudnik tudi posameznik.

Dodatna prednost je izkazano poznavanje eksperimentalnega načrtovanja, anketnega raziskovanja, vedenjskih intervencij ali oblikovanja digitalnih sporočil.

## **4. PONUDBENA CENA**

Pri oblikovanju ponudbene cene ponudnik upošteva vse naloge iz tč. 1.1 tega dokumenta.

## 5. MERILO ZA IZBIRO

Merilo za izbiro najugodnejšega ponudnika je najnižja skupna cena ob izpolnjevanju vseh pogojev in zahtev naročnika.

### DODATNO MERILO V PRIMERU VEČ ENAKOVREDNIH PONUDB:

V primeru, da bosta dva ali več ponudnikov ponudila enako skupno najnižjo ceno, bo izbran ponudnik z večjim številom vsebinsko ustreznih referenčnih poslov. Če bodo ponudniki tudi po tem merilu v enakovrednem položaju, bo izbran ponudnik z žrebom pred strokovno komisijo naročnika.

## 6. NAČIN IN ROK ODDAJE PONUDBE

Ponudnik predloži ponudbo v elektronski obliki (PDF) do 23. 5. 2026 do 15.00 na e-naslov [gp.uiv@gov.si](mailto:gp.uiv@gov.si), z obveznim sklicem »EVN-430-4/2026 - Ponudba«.

Kontaktna oseba za vprašanja v zvezi s predmetnim naročilom je Katarina Janjič, dosegljiva na e-naslovu [gp.uiv@gov.si](mailto:gp.uiv@gov.si).

## 7. PRILOGE

Ponudbi se priložijo reference, opis metodološkega pristopa, predlog ključnih faz izvedbe ter morebitni podatki o podizvajalcih.

## 8. DODATNE INFORMACIJE

### Obseg študije:

Študija se osredotoča na proučitev psiholoških, vedenjskih in komunikacijskih dejavnikov, ki vplivajo na razumevanje, zaznavo, zapomljivost, interpretacijo in upoštevanje sporočil organov s področja informacijske oziroma kibernetne varnosti. Vključevati mora pregled relevantne znanstvene in strokovne literature, analizo vsebinskih in oblikovnih značilnosti sporočil, pripravo analitičnega modela dejavnikov učinkovitosti sporočil ter empirično preveritev ugotovitev na ustreznem vzorcu podjetij oziroma predstavnikov podjetij, ki so naslovniki tovrstnih sporočil.

### Metodologija:

Izvajalec mora metodologijo pred začetkom dela predložiti naročniku v potrditev. Metodologija mora jasno opredeliti raziskovalna vprašanja, vzorec oziroma ciljno skupino, raziskovalne instrumente, način zbiranja podatkov, način obdelave in interpretacije rezultatov ter predvideno kombinacijo kvantitativnih in/ali kvalitativnih raziskovalnih metod. Potrditev metodologije se lahko opravi elektronsko.

### Kakovost in obdelava podatkov:

Izvajalec mora zagotoviti metodološko utemeljenost raziskave, sledljivost uporabljenih virov, ponovljivost postopka ter jasno označiti omejitve, predpostavke in morebitne metodološke zadržke raziskave. Zbiranje in obdelava podatkov morata biti skladna z GDPR in drugimi relevantnimi predpisi.

**Rezultati in oblika oddaje:**

Končni izdelki morajo biti pripravljene v slovenskem jeziku in oddani najmanj v formatih PDF in Word. Preglednice, izvorni podatki, matrike kodiranja in druge priloge morajo biti oddani tudi v strojno berljivi obliki (Excel ali CSV), kadar je to glede na naravo gradiva mogoče. Končni izdelki naj obsegajo najmanj potrjeno metodologijo, pregled literature, raziskovalne instrumente, analitični okvir dejavnikov, končno poročilo s priporočili, nabor praktičnih smernic oziroma kontrolni seznam za pripravo sporočil ter predstavitev ključnih ugotovitev naročniku. Izvajalec mora na končnih izdelkih navesti Urad Vlade Republike Slovenije za informacijsko varnost in po navodilu naročnika dodati logotip.

Dr. Uroš Svete  
direktor urada