



SPOROČILO POSAMEZNIKOM O KRŠITVI VARSTVA OSEBNIH PODATKOV

Zadeva: Pomembno obvestilo o varnostnem incidentu in zaščiti podatkov v aplikaciji UAS repozitorij

Spoštovani operaterji sistemov brezpilotnih zrakoplovov in piloti na daljavo.

V Javni agenciji za civilno letalstvo Republike Slovenije (v nadaljevanju: Agencija) visoko cenimo vaše zaupanje, zato vas želimo transparentno in odprto obvestiti o incidentu, s katerim smo se soočili, ter o ukrepih, ki smo jih nemudoma sprejeli za zaščito vaših podatkov.

Predhodno obveščanje: Kot ste morda že bili seznanjeni, smo vas o prvih ugotovitvah glede incidenta nemudoma obvestili že **16. 4. 2026** z javno objavo na naši spletni strani (www.caa.si) in na našem uradnem Facebook profilu. Tokratno obvestilo podajamo z namenom, da vas seznanimo z ugotovitvami preiskave in dodatnimi varnostnimi ukrepi.

Kaj se je zgodilo? Dne 13. in 14. aprila 2026 je prišlo do nepooblaščenega vstopa v našo spletno aplikacijo UAS repozitorij. Neznani storilec je preko avtomatiziranega dostopa pridobil nepooblaščen vpogled v del podatkovne zbirke. Takoj, ko smo zaznali sum aktivnosti, smo aplikacijo preventivno ugasnili, da bi popolnoma preprečili kakršno koli nadaljnje tveganje ali odtekanje podatkov.

Kateri podatki so bili izpostavljeni? Natančna preiskava je pokazala, da so bili predmet avtomatiziranega dostopa naslednji podatki:

- Osebno ime
- Datum rojstva
- Naslov prebivališča
- E-poštni naslov
- Telefonska številka

Pomembno opozorilo: Finančni podatki, gesla ali občutljivi identifikacijski dokumenti **niso** bili predmet tega incidenta.

Ukrepi, ki smo jih izvedli za vašo varnost

Poudarjamo, da je Agencija situacijo nemudoma prevzela z najvišjo stopnjo resnosti in odgovornosti:

1. **Hitra zamejitev:** V tesnem sodelovanju s **Policijo** in **Uradom RS za informacijsko varnost (URSIV)** smo takoj pristopili k tehničnim in pravnim zaščitnim ukrepom.
2. **Varnostna nadgradnja:** V času, ko je bila aplikacija izključena, so naši strokovnjaki izvedli celovite varnostne nadgradnje sistema in odpravili ranljivosti. Aplikacija je bila po uspešnih testih ponovno varno zagnana dne 28. aprila 2026.
3. **Stalni nadzor:** Po opravljeni preiskavi sicer obstaja sum, da so bili zgoraj navedeni podatki zajeti, vendar poudarjamo, da **se podatki na darknetu (temnem spletu) ali kjerkoli drugje vsaj zaenkrat še niso pojavili**. Situacijo in spletne indikatorje skupaj s pristojnimi organi neprekinjeno spremljamo.



Priporočila za posameznike

Ker so bili izpostavljeni kontaktni podatki (osebno ime, datum rojstva, naslov prebivališča, e-naslov in telefon), vam iz previdnosti svetujemo naslednje specifične zaščitne ukrepe:

- **Bodite pozorni na ciljno usmerjena sporočila (Spear phishing):** Napadalci lahko izpostavljene podatke (ime, naslov, datum rojstva) uporabijo za to, da vas nagovorijo osebno in s tem ustvarijo lažen občutek zaupanja. Če prejmete e-pošto ali dopis, ki vsebuje vaše točne osebne podatke in od vas zahteva plačila, vnose gesel ali potrditev bančnih računov, vedno najprej neodvisno preverite identiteto pošiljatelja (npr. pokličite uradno številko institucije).
- **Spremljajte poslovanje na svojih bančnih računih:** Čeprav finančni podatki niso bili odtujeni, lahko zlonamerni akterji z vašim imenom, naslovom in datumom rojstva včasih poskušajo zavesti podporo strankam pri različnih ponudnikih storitev. Priporočamo redno spremljanje izpiskov in prometa na vaših bančnih računih ter takojšnjo prijavo kakršnih koli nepojasnjenih transakcij.
- **Previdnost pri registraciji novih storitev:** Če opazite kakršna koli potrditvena e-sporočila ali SMS-kodi za storitve, ki jih sami niste odprli ali registrirali, nemudoma kontaktirajte ponudnika te storitve, saj obstaja možnost, da nekdo poskuša uporabiti vaše podatke za ustvarjanje lažnih profilov.
- **Pozornost pri poštnih pošiljkah:** Ker je bil izpostavljen tudi naslov prebivališča, bodite pozorni na nenavadno uradno pošto (npr. opomine za storitve, ki jih niste naročili).
- **Bodite pozorni na e-pošto in SMS sporočila:** Če prejmete splošna sumljiva sporočila neznanih pošiljateljev, ki zahtevajo gesla ali klikanje na povezave, nanje ne odgovarjajte.
- **Preverite identiteto klicateljev:** Če prejmete nenavadne telefonske klice, kjer se osebe predstavljajo v imenu uradnih institucij ali bank in zahtevajo občutljive podatke, klic nemudoma prekinite.

Kontaktni podatki za več informacij

Zavedamo se, da lahko takšne novice povzročijo skrb, zato vam zagotavljamo polno podporo. Za kakršna koli vprašanja, pojasnila ali informacije v zvezi z varstvom vaših osebnih podatkov se lahko kadarkoli obrnete na našo pooblaščen osebo za varstvo osebnih podatkov (DPO):

- **Pooblaščen oseba:** Jaka Kenk
- **E-naslov:** dpo@caa.si

Obžalujemo zaplete, ki so nastali. Sprejeli smo vse potrebne korake, da so naši sistemi postali še bolj robustni, vaša varnost pa ostaja naša glavna prioriteta.

S spoštovanjem,

Javna agencija za civilno letalstvo Republike Slovenije