NOTICE TO INDIVIDUALS REGARDING A PERSONAL DATA BREACH

Subject: Important notice regarding a security incident and data protection in the UAS Repository application

Dear UAS operators and remote pilots,

At the Civil Aviation Agency of the Republic of Slovenia (hereinafter: the "Agency"), we highly value your trust and therefore wish to inform you transparently and openly about an incident we have encountered, as well as the measures we have immediately taken to protect your data.

Previous notification

As you may already be aware, we promptly informed the public of our initial findings regarding the incident on 16th April 2026 through a public notice published on our website and our official Facebook page. The purpose of this notice is to provide you with the results of the investigation and information about additional security measures that have been implemented.

What happened?

On 13th and 14th April 2026, an unauthorized party gained access to our UAS Repository web application. Through automated access methods, the unknown perpetrator obtained unauthorized access to a portion of the database.

As soon as we detected suspicious activity, we proactively shut down the application in order to completely prevent any further risk or potential data leakage.

What data were exposed?

A detailed investigation has shown that the following personal data were subject to unauthorized automated access:

- Full name
- Date of birth
- Residential address
- Email address
- Telephone number

Important notice: Financial data, passwords, and sensitive identification documents were not affected by this incident.

Measures taken to protect your security

We would like to emphasize that the Agency treated this situation with the utmost seriousness and responsibility:

1. Immediate containment

In close cooperation with the Police and the Government information security office of the Republic of Slovenia (URSIV), we immediately initiated technical and legal measures to contain and address the incident.

2. Security enhancements

During the period in which the application remained offline, our experts carried out comprehensive security upgrades and remediated identified vulnerabilities. Following successful testing, the application was securely restored and brought back into operation on 28th April 2026.

3. Continuous monitoring

Although the investigation indicates that the above-mentioned data may have been accessed, we would like to emphasize that, to date, the data have not appeared on the dark web or elsewhere, as far as is currently known. Together with the competent authorities, we continue to monitor the situation and relevant online indicators on an ongoing basis.

Recommendations for individuals

As contact information (full name, date of birth, residential address, email address, and telephone number) may have been exposed, we recommend the following precautionary measures:

- **Be alert to targeted phishing attempts (spear phishing):** Attackers may use exposed information such as your name, address, and date of birth to contact you personally and create a false sense of trust. If you receive an email or letter containing your personal details and requesting payments, passwords, or confirmation of bank account information, always independently verify the identity of the sender (for example, by calling the official contact number of the institution).
- **Monitor your bank accounts and financial activity:** Although financial information was not compromised, malicious actors may attempt to use your name, address, and date of birth to deceive customer support representatives at various service providers. We recommend regularly reviewing your account statements and transaction history and immediately reporting any unexplained transactions.
- **Exercise caution regarding new service registrations:** If you receive confirmation emails or SMS verification codes for services that you did not request or register for, contact the service provider immediately, as someone may be attempting to use your information to create fraudulent accounts.
- **Pay attention to postal correspondence:** As your residential address may have been exposed, be vigilant regarding unusual official mail, such as invoices or payment reminders for services you did not order.

- **Be cautious with emails and text messages:** If you receive suspicious emails or SMS messages from unknown senders requesting passwords or encouraging you to click on links, do not respond and do not interact with the content.
- **Verify the identity of callers:** If you receive unusual telephone calls from individuals claiming to represent government institutions, banks, or other organizations and requesting sensitive information, terminate the call immediately.

Contact information for further information

We understand that such news may cause concern and would like to assure you of our full support. Should you have any questions, require clarification, or need further information regarding the protection of your personal data, please contact our Data Protection Officer (DPO):

- **Data Protection Officer:** Jaka Kenk
- **Email:** dpo@caa.si

We sincerely regret any inconvenience caused by this incident. We have taken all necessary steps to further strengthen the security of our systems, and protecting your information remains our highest priority.

Yours sincerely,

Civil Aviation Agency of the Republic of Slovenia