Continuing the "leakage" of personal data, ie violation of personal data and violation of personal data security of Facebook users, including 650 thousand personal data of Croatian citizens, we would like to inform citizens that AZOP will participate in joint operations and investigations related to this case. a one-stop-shop, together with the Irish Supervisory Authority as the lead supervisor given that Facebook is headquartered in Ireland, and with other interested supervisors, and the public will be informed in good time of the results of the investigation. Also, AZOP will be involved in the investigation regarding the compromise of personal data of LinkedIn users.

We hereby advise citizens to check via the link https://haveibeenpwned.com/ whether their e-mail addresses are compromised, which they use to log in to Facebook, LinkedIn, but also to log in to other social networks, Internet services or services. If they find that a particular email address has been compromised, we suggest the following:

Change the password for this email address to a new strong security password

Create a new separate strong security password for all Internet services and Internet services for which you have used that login email address (e.g. social networks, Internet store, etc.). If this Internet service or service is offered, it would be advisable to include the double authentication option.

A strong security password should include:

16 or more characters (the more the better),

capital letters (ABCDEFGH…),

lowercase letters (abcdefgh (),

figures (34 123456),

symbols (@ # $% {} [] () / \ ‘”,;:. <>…).

Additionally, we warn LinkedIn users not to respond to fraudulent e-mails in which the sender claims to have been sent by LinkedIn's customer service and not to open links contained in such fraudulent e-mails.