



Brussels, 24.6.2025
COM(2025) 342 final

2025/0187 (NLE)

Proposal for a

COUNCIL IMPLEMENTING DECISION

on Authorising Support from the EU Cybersecurity Reserve for Moldova

(Text with EEA relevance)

Proposal for a

COUNCIL IMPLEMENTING DECISION

on Authorising Support from the EU Cybersecurity Reserve for Moldova

(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)¹, and in particular Article 19 (4) thereof,

Having regard to the proposal from the European Commission,

Whereas:

- (1) In its conclusions of 15 December 2022, the European Council affirmed that the Union will continue to provide all relevant support to the Republic of Moldova (Moldova hereafter) as it deals with the multifaceted impact of Russia's war of aggression against Ukraine.
- (2) On 23 June 2022, the European Council granted Moldova the status of candidate country. The decision was based on fulfilment by Moldova of the conditions specified in the Commission's opinion of June 2022 on Moldova's membership application. On 14 December 2023, the European Council decided to open accession negotiations with Moldova, following the recommendation issued by the Commission.
- (3) Cybersecurity incidents continue to cause economic and societal impact both across the Union and at global level. The cyber threats evolve particularly rapidly in some of the EU candidate countries, where possible significant or large-scale incidents can disrupt and damage critical infrastructure, interfere with the proper functioning of its economy and institutions or pose serious public security and safety risks for entities or citizens. This is particularly the case in Moldova where Russia conducts hybrid campaigns and cyber-attacks to threaten critical infrastructure, democratic processes and election infrastructure.
- (4) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not confined to a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to

¹ OJ L 38/2025, 15.1.2025, ELI: <http://data.europa.eu/eli/reg/2025/38/oj>.

the protection of the Union, and particularly its internal market and industry, as a whole. Therefore, Regulation (EU) 2025/38 provides that Digital Europe Programme (DIGITAL) (“DEP”)-associated third countries may be supported from the EU Cybersecurity Reserve (the ‘Reserve’), in all or part of their territories, where this is provided for in the agreement associating the third country to DEP.

- (5) As provided for in Article 19 of Regulation (EU) 2025/38, DEP-associated third countries should be able to request the service from the Reserve when the entities targeted and for which they request support from the Reserve are entities operating in sectors of high criticality or other critical sectors and when the incidents detected lead to significant operational disruptions or might have spillover effects in the Union. The DEP-associated third countries should only be eligible to receive support where the agreement associating them to DEP specifically provides for such support. In addition, such third countries should remain eligible only so long as three criteria are fulfilled. First, the third country should comply in full with relevant terms of that agreement. Second, given the complementary nature of the Reserve, the third country should have taken adequate steps to prepare for significant or large-scale equivalent cybersecurity incidents. Third, the provision of support from the Reserve should be consistent with the Union’s policy towards and overall relations with that country and with other Union’s policies in the field of security.
- (6) The provision of support to the DEP-associated third countries may affect relations with third countries and the Union security policy, including in the context of the Common Foreign and Security Policy and Common Defence and Security Policy. Accordingly, Article 19(4) of Regulation (EU) 2025/38 allows the Council implementing act to specify the time period, which should be no less than 75 days for a single request during which such support can be provided. The Council should act on the basis of a Commission proposal, taking due account of the Commission’s assessment of the three criteria.
- (7) Moldova has been heavily impacted by Russia’s war of aggression against Ukraine, while being also directly targeted by Russia’s hybrid activities, seeking to destabilise the country and undermine its EU path. Against this backdrop, the Union has provided comprehensive support to Moldova in addressing the challenges it faces as a consequence of Russia’s war of aggression against Ukraine, and to strengthen the country’s resilience, security and stability in the face of direct destabilising activities by Russia.
- (8) On 24 April 2023, the Council approved the establishment of a civilian European Union Partnership Mission in Moldova under the Common Security and Defence Policy to provide strategic advice and operational support in the areas of crisis management and countering hybrid threats. Since 2021, the EU has also provided consistent support through the European Peace Facility to strengthen Moldova’s capacities in the military and defence area. The signature of the EU-Moldova Security and Defence Partnership on 21 May 2024 streamlined the structure of EU’s cooperation with Moldova in key areas of peace, security, and defence. Furthermore, the Moldova Growth Plan, adopted by the Commission on 10 October 2024, aims to support Moldova's socio-economic reforms and enhance its access to the EU single market, with specific reforms expected in the area of cybersecurity governance.
- (9) The Commission has assessed the three criteria outlined in Article 19(3) of Regulation (EU) 2025/38 in respect of Moldova and considers them to be fulfilled. It has also

consulted the High Representative of the Union for Foreign Affairs and Security Policy when conducting this assessment,

HAS ADOPTED THIS DECISION:

Article 1

The provision of support from the EU Cybersecurity Reserve to the Republic of Moldova within the meaning of Article 19 of Regulation (EU) 2025/38 is hereby authorised in line with the Commission's proposal, submitted in accordance with Article 19(3) of Regulation (EU) 2025/38.

Article 2

This Decision shall enter into force on the date of its adoption, and shall apply for a maximum of one year.

Done at Brussels,

For the Council
The President