

(English version)

**Question for written answer E-001838/24
to the Commission
Marieke Ehlers (PfE)
(26 September 2024)**

Subject: Protection of classified information within the EU

We MEPs were informed that access to the report from the Commission to the Council on the assessment of third countries' level of cooperation on readmission in 2023 (COM(2024) 340 final) was restricted — as is clearly stated on the document itself.

Nevertheless, we were able to find the document on the Internet, on the Statewatch website. The following questions thus arise:

1. Why do MEPs have to go to a special reading room, without their mobile phones, when the document is openly available online?
2. What safeguards and processes does the Commission use to ensure that restricted documents are not leaked?
3. Is the Commission considering taking action against the Statewatch website and does it strive to ensure that restricted-access EU documents are not published online, whether that be by Statewatch or any other organisation, person or entity?

Submitted: 26.9.2024

**Answer given by Mr Serafin on behalf of the European Commission
(7 January 2025)**

In line with the measures in place to protect classified information, access to such documents is limited on a need-to-know basis, assessed by its originator. Until a document is declassified, the handling rules for the different levels of classification remain applicable.

The unauthorised disclosure of this document on a public website is currently being investigated by the relevant security services.

With a view to ensuring the necessary protection of such information, the Commission has put well calibrated mitigating measures in place, such as robust security policies, procedures, infrastructures and security awareness measures.

The Commission makes relentless efforts to enshrine a solid security culture and cooperates with the other EU institutions and the national competent authorities entrusted with investigative powers in case of incidents.

While the Commission does not generally target specific websites, it actively monitors and, if necessary, responds to unauthorised disclosures of sensitive information across various platforms and takes necessary measures.
