Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 13 February 2026

WK 2399/2026 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV
COMPET
MI

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Omnibus VII (Digital Omnibus) – Follow-up to the AGS of 13 February – Presentation by the Commission on cybersecurity issues

Following the meeting of the Antici Group (Simplification) of 13 February 2026 on Omnibus VII (Digital Omnibus), delegations will find attached the presentation shown by the Commission regarding cybersecurity issues.

European Commission

PUBLIC

DIGITAL OMNIBUS

Antici Group on Simplification

13/2/2026

Cybersecurity

Single-entry point for incident reporting

Debrief from the 2nd Technical Workshop on SEP – 4 February 2026

- COM and ENISA organised 2 workshops focused on technical questions (on 28/11/2025 and 04/02/2026)
- In the 2nd workshop on 4 February - over 150 participants from MS - online and in person (from AGS, HWPCI, CSIRTs, NCAs)
- ENISA presented possible technical solutions for the single-entry point for incident notifications - based on the case study paper shared by Poland within AGS

Main take aways from the 2nd technical workshop

- It is technically possible to cater for various solutions to address various legal requirements and MS national specificities.
- *Security of SEP*: security safeguards, various solutions for data storage possible, including no central data storage -> no single point of failure.
- Preserve *trusted relationship* and direct interaction with national authorities: possibilities for SEP integration of national platforms, where they are in place (gained trust of reporting entities).
- Authentication solutions when using SEP, taking account of national solutions; possibility to use digital identity wallets and business wallets;
- Possibility for entities to retrieve and supplement information; possibility to fill in information in different stages, as per specific reporting requirements, including national;
- Preserving possibility for follow up actions by NCAs after incident report, e.g. assigning case number, providing assistance;
- Need to find technical solutions for languages used and built-in translation tools;
- Importance of adopting common templates for NIS2 reporting; alignment with DORA, GDPR etc, to the extent possible.

Replies to further questions and comments from MS

SEP development process and timeframe

- ENISA shall develop the SEP within 18 months from the entry into force of the Digital Omnibus Regulation.
- ENISA shall pilot the functioning of the SEP for each added Union legal act.
- COM, in cooperation with ENISA, shall assess the proper functioning, reliability, integrity and confidentiality of SEP.

  If positive assessment – COM publishes a notice; SEP ready to proceed.

  If not positive assessment – ENISA, in cooperation with COM, shall take corrective measures without undue delay. COM reassesses and publishes notice.
- The obligations to report via the SEP enter into application 18 months from the entry into force of the Digital Omnibus Regulation.
- When COM finds in its assessment that the SEP does not ensure the proper functioning, reliability, integrity or confidentiality, term of application can extend to 24 months.

Active role of Member States in the process

- Member States would be part of the process during all phases, i.e. in the design, development, piloting, testing and assessment before the SEP becomes operational:
  - ENISA to consult MS (CSIRTs network and competent authorities) when drafting the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the SEP on the points listed in *Art 23a(3).*
  - ENISA to consult competent authorities before piloting the functioning of the SEP (e.g. on the specificities and requirements for the notifications for a specific Union legal act that should be considered for the test)
  - COM to consult MS (CSIRTs network and competent authorities) on the proper functioning, reliability, integrity and confidentiality of the SEP (e.g. by consulting them on the assessment methodology and findings).
  - ENISA and COM to make use of existing cooperation groups and networks of Member States

Security of SEP and preserving trust

- Important to retain the trusted relationship between relevant authorities and reporting entities
  - The SEP should not affect trust building efforts between authorities and reporting entities and follow-up exchanges that help handling incidents. It does not interfere with the interaction between businesses and relevant authorities.
  - The SEP merely provides a tool/conduit to facilitate compliance with legal reporting obligations. Direct communication channels with MS authorities will be preserved.
  - The aim of the comprehensive consultation and cooperation process building up the SEP is to ensure that the SEP is a workable solution for MS and businesses alike and that it factors in the specificities it needs to be adjusted to.
  - MS should also advise ENISA and COM on their stakeholders' perspective and specific needs to ensure that notifying entities have trust in the SEP and ensure a user-friendly experience.

MS comments on security and development of SEP

- **Security of SEP**: Ensuring adequate technical and security requirements are put in place (preparatory study, security audits, piloting and testing)
- **Integration of existing national platforms** should be possible and reflected in technical build-up; preparatory study and piloting phase can identify issues and mitigate risks of delays in onboarding
- **Governance model**: involvement of MS in all steps of SEP design and development
- **Trigger of an extension for onboarding**: where COM finds that SEP does not ensure the proper functioning, reliability, integrity or confidentiality.

Processing of personal data and application of EU data protection rules

- Based on the agreed architecture of SEP: it would depend which personal data are processed in the context of the SEP (e.g. of the employee of the controllers submitting the notification) and who is accessing/processing it.
- As a general rule, when the NCAs are processing the data, the GDPR would apply; if any relevant personal data would be controlled or processed by ENISA, the EUDPR would apply.

Financing of SEP

- SEP cost calculation methodology in SWD
  - **For ENISA** (budgetary implications under CSA2/ENISA mandate): initial development cost of EUR 6 million + EUR 500k for onboarding of any additional legal act + 8 FTE for maintenance (based on CRA SRP experience; see also ESAs Report under Art 21 DORA)
  - **For Member States**: building a national platform (for reporting under 2 or 3 legal acts only). Depending on the type of solution, initial set up costs were estimated to range from EUR 150,000–200,000 up to EUR 1.3–1.5 million per MS; for more complex solutions potentially higher + additional maintenance costs, including 2-4 FTEs per MS.

- With an EU legislation establishing a SEP, in addition to ENISA's budget, EU funds could support the development and implementation of the project.