



Council of the
European Union

Brussels, 15 February 2023
(OR. en)

5601/23

LIMITE

**COSI 27
ENFOPOL 64
IXIM 28
CATS 10
COPEN 37
CYBER 32**

NOTE

From:	Presidency
To:	Delegations
Subject:	Proposal to establish a High-Level Expert Group on Access to Data

1. INTRODUCTION

At the Informal meeting of justice and home affairs on 26 January 2023, under the agenda point ‘Going Dark’, ministers discussed the challenges judicial and law enforcement agencies face in the digital era in effectively accessing relevant data in order to fight crime. These challenges include, inter alia, the need for effective approaches to access encrypted communications, the need for enhanced international cooperation to ensure access to evidence due to the inherent cross-border nature of digital services, the need for a clear framework for data retention, the increased need for effective instruments and methods to address the volatility of electronic information, and the jurisdictional concerns engendered by the loss of location.

The aggregated result of these challenges is that, in the absence of an appropriate response, law enforcement's mission to fight crime and terrorism as enshrined in law, is seriously impeded. Tools for judicial and law enforcement purposes can often no longer be applied due to developments such as the use of encryption technologies. Unless new approaches are developed, the ability of judicial and law enforcement agencies to effectively prevent, detect, investigate and prosecute crime will continue to fall further behind digital developments, creating a risk for impunity in digital environments, and therefore in real life.

The issue of access to data has been discussed for a long time, but these discussions have mainly been conducted in a compartmentalised manner. It is time to take stock from a wider perspective, including on the balance to be struck between the right to privacy and the right to security.

Proposal to establish a High-Level Expert Group on Access to Data

At the informal meeting of justice and home affairs ministers, the Presidency's proposal to establish a new forum gathering all relevant actors to jointly and comprehensively take forward the issue of effective lawful access to data received broad support among ministers. The ministers tasked COSI to develop the concrete follow up on this matter.

Against this background, the Presidency proposes to establish a High-Level Expert Group (HLEG), gathering stakeholders from all relevant sectors thereby enabling a comprehensive and joint effort to define the challenges related to access to data and to recommend measures to address them. The Presidency believes that the establishment of a HLEG is needed to enhance and facilitate EU-action to improve access to data, electronic evidence, and information for judicial and law enforcement purposes. The HLEG on information systems and interoperability was key in overcoming the previously prevailing silo approach and proposing concrete ways forward. This positive experience could serve as inspiration to address the similarly cross-cutting issue of access to data.

While access to data has been discussed in many forums for a long time, including several successful initiatives from preceding council presidencies, the Presidency intends for the HLEG to include actors from all relevant sectors, and to propose recommendations to solve concretely defined problems. The message that the Presidency wants to convey is that data access is not a concern for judicial and law enforcement authorities alone, but an issue that concerns all stakeholders in the digital environment. For the same reason, the Presidency believes that the HLEG format would allow going beyond the Council and its working structures, thus enabling a broader participation of various stakeholders. The HLEG should benefit from the work already conducted by, for example, the EU Internet Forum, the EU Innovation Hub and the Commissions' work on the way forward on encryption. The HLEG should have a clear mandate, limited in time, avoiding to duplicate work conducted elsewhere.

Next steps: The purpose of the discussion in COSI on 22 February is to agree on the way forward to establish a HLEG and to hold a first exchange of views about the objectives, format, and basic organisational aspects of such a forum. Based on the input from delegations, the Presidency together with the Commission will draft an outline of the main challenges and a mission description including expected outputs and basic organisational aspects of the HLEG, to be submitted to the Commission. This scoping paper will be brought to the attention of COSI at an upcoming meeting.

2. PROPOSED CONTENT AND EXPECTED OUTCOMES

The Presidency proposes to mandate the HLEG to analyse and propose solutions to the issue of communication data as a necessary measure to safeguard the prevention, detection, investigation, or prosecution of criminal offences. The work of the HLEG should result in recommendations for legislative, non-legislative or practical measures and the development of joint and coherent approaches on the issues at hand. To present concrete recommendations, topics should be clearly defined and addressed in specialised sub-groups.

The work of the HLEG should be guided by a comprehensive horizontal approach that considers the need to uphold all fundamental rights in digital environments as well as the need to guarantee information security and cybersecurity, while allowing judicial and law enforcement authorities' continued lawful access to digital data in the performance of their duties.

3. ORGANISATIONAL ASPECTS

The Presidency invites COSI to consider the following aspects of a HLEG

a) Format

The Presidency suggests to establish a HLEG to enhance and facilitate a common EU response in improving access to communications data as a necessary measure to safeguard the prevention, detection, investigation, or prosecution of criminal offences. The HLEG may be supported by expert-level subgroups, for the purpose of examining specific questions.

b) Chairmanship, reporting and timeline

The Presidency proposes to ask the Commission to consider setting up the HLEG, further to guidance provided by COSI on its tasks and practical arrangements of its work. The HLEG could be co-chaired by the Presidency and the Commission, who will act jointly as driving forces behind the initiative.

The HLEG should report regularly to COSI on its findings and present the result of its work to the committee. The HLEG should present the result of its work by mid-2024. The timelines for each subgroup may vary according to their respective area of focus and should report to the high-level group accordingly.

c) Participants

The Presidency is of the view that the HLEG should be able to involve all relevant stakeholders, to break the silo approach and take steps toward a joint understanding of the issue of access to data. Alongside the Member states practitioner, the HLEG should also include input from a wider range of participants with specific expertise on a subject on the agenda, to take part in the work of the group or sub-groups on an ad hoc basis. Such wider participation could include representatives from the European Parliament, academia, representatives of the industry (e.g., cybersecurity, telecommunication operators and Over the Top service providers) and representatives of non-governmental organizations.

Questions for discussion

1. Do you agree with the Presidency's proposed way forward to address the issue of enhanced access to data for judicial and law enforcement authorities? In your opinion, which are the main areas and challenges that should be the primary focus of the HLEG and/or its sub-groups? And what specific operational or other challenges do authorities in your Member State face when it comes to access to data for the purposes of enforcing the legal framework?
 2. Do you agree the group should be co-chaired by the Commission and the Presidency?
 3. Do you agree that the HLEG should involve also non-institutional actors, as appropriate?
 4. Can the HLEG benefit from synergies with existing structures and forums and ongoing work related to access to data? If yes, in what way?
-