



EUROPEAN COMMISSION
Directorate-General for Migration and Home Affairs
Directorate Internal Security

Directorate-General for Communication Networks, Content and Technology
Directorate Digital Society, Trust and Cybersecurity

INFORMAL COMMISSION EXPERT GROUP FOR A TECHNOLOGY ROADMAP ON ENCRYPTION
TERMS OF REFERENCE

1. BACKGROUND

In June 2023, the Swedish Presidency of the Council, in cooperation with the Spanish, Belgian and Hungarian Presidencies and with the support of the European Commission, proposed and organised, a High-Level Group (HLG) on Access to Data for Effective Law Enforcement. Its objective was to address current law enforcement challenges and anticipate future ones, against the background of technological developments. The HLG published its final report in November 2024¹, which was subject to Council conclusions² in December 2024.

The HLG experts representing law enforcement have identified encryption among the main challenges they face. The HLG report recognises that encryption plays a fundamental role in ensuring cybersecurity and privacy. HLG experts also highlighted the necessity to have lawful access to data in a readable format in the course of a criminal investigation, in a targeted manner, ensuring strong cybersecurity, in full respect of fundamental rights and subject to appropriate safeguards.

The report suggests in several instances to address those challenges through “a Technology Roadmap that brings together technology, cybersecurity, privacy, standardisation and security experts and ensures adequate coordination³.” Experts also suggest that “the Technology Roadmap for Lawful Access should set objectives and frame activities with associated funding to achieve those objectives with a view to anticipate technological challenges through a comprehensive and forward-looking policy”.

To meet this objective, the Commission is setting up an expert group **to deliver a technology roadmap on the challenges of encryption in the context of criminal investigations** (referred to as “the Technology Roadmap”). The Technology Roadmap should be delivered within 12 months after its creation, and subsequently presented to relevant stakeholders.

The group should focus on current and future **technical challenges** impacting lawful access to digital information in the context of criminal investigations. The work should notably focus on **fixed and mobile communications and devices, where lawful access to data is impacted by**

¹https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en

² <https://www.consilium.europa.eu/en/press/press-releases/2024/12/12/access-to-data-council-calls-for-challenges-for-law-enforcement-to-be-addressed/>

³ From recommendation 22 of the “Recommendation report of the High Level Expert Group on Access to Data.”

encryption. It should also address encryption in the context of digital forensics and of data retention.

In that context, “*lawful access to data*” means the access to digital information law enforcement authorities need for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Such access needs to be necessary and proportionate for these purposes and should not undermine data protection, privacy and cybersecurity. It should be based on clear, precise and accessible rules set out in law, subject to oversight mechanisms, and with effective remedies provided for the individuals that may be affected by the access to their data.

The group should identify potential technical options and assess their suitability to improve lawful access to data by law enforcement, in full respect of fundamental rights as well as existing relevant case law and without undermining cybersecurity. The group should focus on technologies that are already available or possibly developed in the future to ensure lawful access to data. Such technologies should comply with the legal requirements of lawful access, including being able to target the access to specific data and individuals, to ensure its necessity and proportionality with the purposes pursued; maintaining the level of cybersecurity for users; and ensuring the application of adequate oversight mechanisms and remedies for affected individuals, in compliance with privacy and data protection rules and without undermining cybersecurity.

When assessing the impact of such technologies on cybersecurity, the technology roadmap should examine the risks these technologies present, including risks posed by sophisticated nation state threat actors and technical, behavioural, and organisational risk factors. The technology roadmap should also consider technical and organisational measures to address, mitigate and possibly remedy such risks.

2. SUBJECT MATTER

The Informal Expert Group “*Expert Group for a Technology Roadmap on Encryption*” (‘the group’) is set up.

3. TASKS

The group’s tasks shall be:

- to assist the Commission’s Directorate-General for Migration and Home Affairs (‘DG HOME’) and Directorate General for Communications Networks, Content and Technology (‘DG CNECT’) in the preparation of policy initiatives on lawful access to data through the identification of technical options to address encryption challenges and the assessment of their suitability; while ensuring observance of fundamental rights, including privacy and data protection, and without undermining cybersecurity.
- to assist the Commission to elaborate a Technology Roadmap, by providing expert input that shall outline and assess the technical options as well as the corresponding resources and actions needed for lawful access to and processing of digital information, without

undermining cybersecurity and while respecting fundamental rights, taking into account the relevant recommendations of the High-Level Group of Experts for Access to Data⁴.

More specifically, with regard to the Technology Roadmap, the group shall set out and, where applicable, provide a timeline for:

- **the identification of tools** that law enforcement authorities currently need and will need in the future to find, retrieve and analyse data in encrypted environments in a way that is compatible with the applicable EU legal framework (notably the Law Enforcement Directive (LED), the ePrivacy Directive, the General Data Protection Regulation (GDPR) and when relevant the AI Act) and that do not undermine cybersecurity. Such tools shall facilitate digital forensics, decryption, remote data collection, and crime analysis activities. In the absence of available tools, recommendations for the development of those tools should be developed, setting out specific steps accompanied by a timeline.
- **the identification of technological solutions that ensure that future information and communication technologies (such as 6G or quantum encryption) do not negatively impact the ability of law enforcement authorities to have lawful access to data, while guaranteeing compliance with fundamental rights and without undermining cybersecurity.** In the absence of available tools, the Technology Roadmap shall provide recommendations for the development of such technologies, as well as of related standards, in a manner compatible with legal obligations defined on access to data in the context of criminal investigations. Those measures shall not undermine cybersecurity for users.
- specific actions to foster **research into and development and uptake of tools** for data acquisition and access to data, including decryption capabilities;

The outcomes of the technology roadmap may also inform specific actions to foster a **coordinated approach to standardisation** as well as work to develop a **methodology to develop, handle and use targeted lawful access** to address cases where access to data is not possible through cooperation with electronic communications services providers.

The group shall apply the following methodology:

- **1st step: identifying technical options**, including a mapping of current capabilities, that enable lawful access without undermining cybersecurity, including encryption, and complying with legal requirements, including fundamental rights (including privacy and data protection).
- **2nd step: assessing the suitability of the options** identified in the 1st step in light of their effectiveness to improve lawful access to data by law enforcement authorities, in compliance with fundamental rights (as required by the EU Charter of fundamental rights, secondary legislation, and the case law of the CJEU) and their ability to maintain cybersecurity.
- **3rd step: providing concrete and specific recommendations on the implementation and the development of capabilities and standards** based on the (existing or future)

⁴ Notably recommendations 4, 10, 15, 16, 20, 22, 23 and 24, Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, May 2024, available at https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en.

technical options assessed in the 2nd step as meeting the objectives of lawful access, fundamental rights and cybersecurity.

4. CONSULTATION

DG HOME and DG CNECT may consult the group on other matters relating to encryption and lawful access to data in criminal investigation pertaining to its mandate.

5. MEMBERSHIP

1. The group shall be composed of a maximum of 15 members. Of these:
 - a) No more than 12 individuals appointed in a personal capacity with proportional representation of the following fields of expertise: home affairs (covering the area of digital forensics, data retention and lawful interception); cybersecurity (with diverse backgrounds including but not limited to vulnerability management, evaluation of cybersecurity risks and certification and encryption (including quantum); telecommunication (including 5G/6G and messaging applications), big data analysis; standardization; justice and fundamental rights (including data protection and privacy); Cross-cutting expertise as well having an industrial background in relation with technology development shall be an asset.
 - b) ENISA, EUROPOL and the EDPS.
2. Members appointed in a personal capacity shall act independently and in the public interest.
3. ENISA, Europol and the EDPS shall nominate their representatives and shall be responsible for ensuring that their representatives provide a high level of expertise.
4. Members who are no longer capable of contributing effectively to the expert group's deliberations, who, in the opinion of DG CNECT and DG HOME, do not comply with the conditions set out in Article 339 of the Treaty on the Functioning of the European Union or who resign, shall no longer be invited to participate in any meetings of the group and may be replaced for the remainder of their term of office.

6. SELECTION PROCESS

1. The selection of the group's members as referred to in section 5.1.a) shall be carried out via a public call for applications, to be published on the Register of Commission expert groups and other similar entities ('the Register of expert groups'). In addition, the call for applications may be published through other means, including on dedicated websites. The call for applications shall clearly outline the selection criteria, including the required expertise in relation to the work to be performed. The minimum deadline for applications shall be four weeks.
2. Individuals applying to be appointed as members of the group in a personal capacity shall disclose any circumstances that could give rise to a conflict of interest. In particular, the Commission shall require those individuals to submit a declaration of interests ('DOI') form on the basis of the standard DOI form for expert groups⁵, together

⁵ C(2016)3301, Article 11 and Annex 4.

with an updated *curriculum vitae* (CV), as part of their application. Submission of a duly completed DOI form shall be necessary in order to be eligible to be appointed as a member in a personal capacity. The conflict of interest assessment shall be performed in compliance with the Commission's horizontal rules on expert groups ('the horizontal rules')⁶.

3. The members of the group shall be appointed by the Directors-General of DG CNECT and DG HOME; for the experts as referred to in point 5.1.a), from applicants with competence in the areas referred to in point 3 and who have responded to the call for applications, and, for the experts as referred to in point 5.1.b), from applicants with competence in the areas referred to in point 3 proposed by ENISA, EUROPOL and the EDPS, respectively.
4. Members shall be appointed for an initial fixed term of 12 months. Each member's appointment can be renewed for further terms of 12 months each if the appointed expert possesses the necessary expertise for subsequent tasks assigned to the group by DG HOME and DG CNECT after completion of the Technology Roadmap. If after 12 Months different expertise is required, new members shall be selected to replace existing members with less relevant expertise. The selection of new members shall take place via an open call for applications as set out in paragraph 1. Members shall remain in office until replaced, without prejudice to point 5(4).
5. The Directors-General of DG HOME and DG CNECT shall appoint alternate members, in accordance with the same conditions as members, who shall automatically replace any members who are absent or indisposed.
6. The Directors-General of DG CNECT and DG HOME shall establish a reserve list of suitable candidates that may be used to appoint members' replacements. Applicants shall be asked for their consent before including their names on the reserve list.

7. CHAIR

The group shall be co-chaired by a representative of DG CNECT and a representative of DG HOME.

8. OPERATION

1. The group shall act at the request of its co-Chairs with the agreement of DG CNECT and DG HOME, in compliance with the horizontal rules⁷.
2. Meetings of the group shall, in principle, be held on Commission premises or virtually, depending on the circumstances.
3. DG CNECT and DG HOME shall provide secretarial services.
4. Commission personnel from DG CNECT and DG HOME and from other departments with an interest in the proceedings may attend meetings of the group.
5. In agreement with DG CNECT and DG HOME the group may, by simple majority of its members, decide that deliberations shall be public.

⁶ Idem.

⁷ C(2016) 3301, Article 13.1.

6. Minutes on the discussion on each point on the agenda and on the opinions delivered by the group shall be meaningful and complete. Minutes shall be drafted by the secretariat under the responsibility of the co-Chairs
7. As far as possible, the group shall adopt its opinions, recommendations or reports by consensus. In the event of a vote, the outcome of the vote shall be decided by simple majority of the members. Members who have voted against or abstained shall have the right to have a summary of the reasons for their position annexed to the opinions, recommendations or reports.

9. INVITED EXPERTS

DG CNECT and DG HOME may invite experts with specific expertise, including from industry and from civil society, with respect to a subject matter on the agenda to take part in the work of the group on an *ad hoc* basis.

10. OBSERVERS

1. Public entities other than Member States' authorities may be granted an observer status, in compliance with the horizontal rules, by direct invitation.
2. Public entities appointed as observers shall nominate their representatives.
3. Observers and their representatives may be permitted by the Chair to take part in the discussions of the group and provide expertise. However, they shall not participate in the formulation of recommendations or advice of the group.

11. RULES OF PROCEDURE

On a proposal by and in agreement with DG CNECT and DG HOME the group shall adopt its rules of procedure by simple majority of its members, on the basis of the standard rules of procedure for expert groups, in compliance with the horizontal rules⁸.

12. PROFESSIONAL SECRECY AND HANDLING OF CLASSIFIED INFORMATION

The members of the group and their representatives, as well as invited experts and observers], are subject to the obligation of professional secrecy, which by virtue of the Treaties and the rules implementing them applies to all members of the institutions and their staff, as well as to the Commission's rules on security regarding the protection of Union classified information, laid down in Commission Decisions (EU, Euratom) 2015/443⁹ and 2015/444¹⁰. Should they fail to respect these obligations, the Commission may take all appropriate measures.

⁸ C(2016)3301, Article 17.

⁹ Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).

¹⁰ Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

13. TRANSPARENCY

1. The group shall be registered in the Register of Commission expert groups and other similar entities ('the Register of expert groups').
2. As regards the group composition, the following data shall be published on the Register of expert groups:
 - (a) the name of individuals appointed in a personal capacity;
 - (b) The name of observers, if any.
3. All relevant documents, including the agendas, the minutes and the participants' submissions, via the Register of Expert Groups. In particular, DG CNECT and DG HOME shall publish the agenda and other relevant background documents in due time ahead of the meeting, followed by timely publication of minutes. Exceptions to publication shall only be possible where it is deemed that disclosure of a document would undermine the protection of a public or private interest as defined in Article 4 of Regulation (EC) N° 1049/2001¹¹.

14. MEETING EXPENSES

1. Participants in the activities of the group shall not be remunerated for the services they offer.
2. Travel and subsistence expenses incurred by participants in the activities of the group shall be reimbursed by the Commission. Reimbursement shall be made in accordance with the provisions in force within the Commission and within the limits of the available appropriations allocated to the Commission departments under the annual procedure for the allocation of resources.

15. DURATION

The expert group input for the Technology Roadmap shall be delivered no later than 12 months after the creation of the group. The Commission will re-assess the mandate of the group and the possible continuation of its work following the delivery and presentation of the Technology Roadmap.

Done in Brussels, on 26 June 2025

¹¹ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, p. 43–48.