Recommendations
of the High-Level Group
on Access to Data for Effective Law Enforcement

The opinions expressed are those of the experts only and should not be considered as representative of the European Commission's official position.

Introduction

The European Union constitutes an area of freedom, security, and justice with respect for fundamental rights and for the different legal systems and traditions of the Member States.[1] It endeavours to ensure a high level of security through measures to prevent and combat serious and organised crime, including strengthening cross-border law enforcement and judicial cooperation[2], excluding any interference with national security, which remains under the exclusive competence of the Member States. To ensure an effective approach to fighting crime and other challenges related to maintaining a high level of security, law enforcement authorities need to be able to carry out their tasks effectively and lawfully and in full respect of fundamental rights to prevent, detect and investigate criminal offences and ensure their prosecution, to serve justice in the general interest and in particular of that of victims, and to safeguard public security.

[1] *The Treaty on The Functioning of the European Union* (TFEU), Article 67, para 1.
[2] *Ibid.*, para 3.

In recent years, despite the creation, transmission and storage of ever greater quantities of data, access to data for law enforcement purposes has emerged as a key challenge to carry out investigations and prosecutions into criminal offences and to effectively enforcing law. The EU has put in place strong rules to facilitate cross-border access to electronic evidence (the "EU e-evidence rules").[3] However, the absence of data retention obligations negatively affects the effectiveness of e-evidence rules, as there is no guarantee that all the information subject to European preservation or production orders, including traffic data, data requested for the sole purpose of identifying the user, and subscriber data, is available. Moreover, the EU e-evidence rules cover solely data in possession of service providers and do not address the challenge of encryption. Therefore, without operative measures for lawful access to data, this risks to fall short in ensuring effective law enforcement. For the purposes of this document, access to data is understood as access granted to law enforcement, subject to *ex ante* judicial authorisation when required, for the purposes of criminal investigations and on a case-by-case basis. As a rule, in the cases where such judicial authorisation is necessary due to the sensitive nature of the data in question, it represents an integral part of the applicable legal and operational framework. Access to data must be achieved in full respect of fundamental rights, as well as in relation to the case-law of the Court of Justice of the European Union (CJEU) and of the rulings by the European Court of Human Rights on these matters, and applicable procedural safeguards.

This challenge has long been on the political agenda. Inter alia, the European Council, the Council,[4] the European Parliament,[5] the CJEU, and EU agencies have on several occasions discussed and formulated conclusions on various legal and policy aspects of access to electronic communications data, including traffic and location data (metadata), and more generally to electronic evidence. Already in its conclusions of 22–23 June 2017,[6] the European Council called for "addressing the challenges posed by systems that allow terrorists to communicate in ways that competent agencies cannot access, including end-to-end encryption, while safeguarding the benefits these systems bring for the protection of privacy, data and communication" and highlighted that "effective access to electronic evidence is essential to combating serious crime".

---

3 *See E-evidence - cross-border access to electronic evidence - European Commission (europa.eu). The new rules will enter into force on 17 August 2023 and will apply as of 17 February for the Directive and 17 August 2026 for the Regulation.*

4 8289/1/16, *Council conclusions on improving criminal justice in cyberspace.*

5 OJ 2018/C 346/29, Eu*ropean Parliament resolution of 3 October 2017 on the fight against cybercrime.*

6 EUCO 8/17.

The EU Strategy to tackle Organised Crime 2021–2025 stresses the importance of access to electronic communications data to tackle organised crime and of making law enforcement and the judiciary fit for the digital age.[7] Access to data is also of key importance for all EMPACT priorities in the fight against serious and organised crime for 2022–2025,[8] and the EU Security Union Strategy has stated that the Commission will explore measures to enhance law enforcement capacity in digital investigations.[9] In 2023 the Swedish Council Presidency presented the document 'Law Enforcement – Operational Needs for Lawful Access to Communications (LEON[10])' which sets out a comprehensive list of operational needs of law enforcement authorities with respect to communications networks and services.[11]

To identify possible ways forward, the Swedish Presidency, in cooperation with the subsequent Spanish and Belgian Presidencies, initiated the High-Level Group on access to data for effective law enforcement (HLG), composed of high-level representatives of the Member States, the Commission, relevant EU bodies and agencies, and the EU Counter-Terrorism Coordinator, in June 2023[12]. It is co-chaired by the Commission and the rotating Presidency of the Council of the EU and has explored challenges that law enforcement practitioners in the Union face in their daily work in connection to access to data, and has identified potential solutions and recommendations to overcome them, with the aim of ensuring the availability of effective law enforcement tools to fight crime and enhance public security in the digital age, in full respect of fundamental rights.

---

7 *Communication from the Commission on the EU Strategy to tackle Organised Crime 2021–2025*, COM/2021/170 final of 14 April 2021.

8 8665/21.

9 *Communication from the Commission on the EU Security Union Strategy,* COM/2020/605 final of 24 July 2020

10 LEON is the outcome of work undertaken by Swedish law enforcement agencies, in close co-operation with law enforcement representatives in EU Member States, North America and Australia. The aim is to identify and describe the law enforcement needs for lawful access to communications content, content related data and subscriber information.

11 *Communication from the Council Presidency on Law Enforcement Operational Needs for Lawful Access to Communications (LEON),* 6050/23 of 16 February 2023

12 *Commission decision setting up a high-level group on access to data for effective law enforcement*, C(2023) 3647 of 6 June 2023

Throughout its work, the HLG identified ample evidence of and repeatedly conveyed the persistent -if not growing- lack of effective access to data. Moreover, further evidence is still being collected through targeted consultations. Digitally generated, processed, or stored communication data (both metadata and content data) is an important component of modern criminal investigations.[13] As criminals rely more and more on online services, requests for data to online service providers have tripled between 2017 and 2022.[14]

The HLG maintains that law enforcement authorities face increasing operational challenges when seeking to lawfully access data digitally generated, processed or stored in a readable format. 47% of respondents to the most recent annual survey of the SIRIUS project on Cross-Border Access To Electronic Evidence identified the lack of data retention as the predominant challenge they faced,[15] and already in 2018 it was estimated that by 2019 more than 22 percent of global messaging was estimated to be end-to-end encrypted and inaccessible to law enforcement.[16] The HLG identified the lack of an adequate legal framework to perform lawful interception on non-traditional telecommunications services to also have significant consequences for law enforcement action: more than 90% of messaging passes through such Over-The-Top (OTT) services.

To address these challenges, the HLG has formulated strategic, forward-looking recommendations to address current and anticipated challenges against the background of technological developments, enabling a comprehensive EU approach to ensure access to data for effective law enforcement. These recommendations were formulated by the experts of the working groups of the HLG, who were selected by Member States and relevant EU bodies and agencies. Experts included mainly representatives of law enforcement and judicial authorities, but also cybersecurity practitioners and data protection experts.

---

[13] Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.{COM(2018) 225 final} - {COM(2018) 226 final} - {SWD(2018) 119 final}

[14] 2023 SIRIUS Report, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, p. 69.

[15] Ibid, p. 46.

[16] https://www.csis.org/blogs/strategic-technologies-blog/scoping-law-enforcements-encrypted-messaging-problem.

The recommendations that follow in this report were formulated around the three use-cases around which the working groups were organised. Recommendations have been grouped under the relevant workstream and have been endorsed by the HLG at its 4th Plenary on 21 May 2024. These recommendations will be operationalised and will undergo an assessment of legal, technical and financial feasibility, bearing in mind the limited budgetary and human resources available under the EU budget, in a second phase, with a view to providing a concluding report in autumn 2024.

Main drivers to the recommendations

The input reflected above, as well as detailed discussions in three HLG Plenary meetings, nine expert group meetings, a public consultation meeting, and written contributions, allowed the identification of key problem drivers that underpin the challenges set out above and provide a rationale for the recommendations.

Regarding **access to data at rest in a user's device**, the HLG identified as main issues: the lack of cross-border law enforcement cooperation concerning the sharing of digital forensic tools; the insufficient cooperation between law enforcement and the relevant providers, manufacturers and suppliers of hardware and software, hampering the ability to access the data in clear; the difficulty to gain lawful access to a user's device and, if access is possible, extracting and decrypting the data and metadata available to obtain intelligible information that can be of use to investigations and presented as admissible evidence in court.

The HLG considers the pace of technological developments related to **encryption** of information on devices to be rapid to the point that existing decryption tools and techniques are becoming ineffective. This is especially true in cases where suspects and organised crime groups make use of specifically designed communication devices and networks. The time required to decrypt data extracted from devices is also a significant issue: experts reported that this might take up to two years in some instances. The degree of difficulty involved in decrypting bespoke devices that have been designed and marketed exclusively for criminal purposes is even higher and presents further challenges to digital forensics departments across the Member States.

However, it is important that technical solutions to enable authorities to use their investigative powers preserve all the advantages of encryption for data protection, privacy, cybersecurity, and national security reasons. This principle of 'security through encryption and security despite encryption' was a central tenet of the HLG discussions, and future technical solutions or tools that are developed must not result in the weakening or undermining of encryption technologies for the communication of other users that is not subject to the lawful access measure.

A key issue raised by the HLG is the **lack of cross-border law enforcement cooperation mechanisms** concerning the sharing of digital forensic tools between Member States, as these often have distinct solutions for similar technical problems. Despite Europol hosting an in-house repository for tools that can be accessed and used by national law enforcement authorities, Member States likely have access to further tools and bespoke decryption software. However, they refrain from sharing these, either due to a lack of trust and communication between the relevant digital forensic departments or because they are not allowed to do so by law, often due to national security concerns.

The HLG agreed that **networks** such as the European Network of Forensic Science Institutes (ENFSI[17]) dedicated to coordination and knowledge-sharing of digital forensic methods, tools, and best practices, are key for digital forensic practitioners across the EU. Such networks already exist, but to improve communication and collaboration between the digital forensic departments of different Member States they should be further supported and mapped to foster both increased knowledge and tool sharing,[18] supported by a centralised system. The HLG also outlined that the cost of commercial digital forensic tools was a significant barrier faced across Member States, and that there ought to be further research and tool development carried out at the EU level and the use of already existing mechanisms, such as the European Anti Cybercrime Technology Development Association (EACTDA) and the Europol Tool Repository for their dissemination.[19] The evaluation and certification of commercially available tools was a further recurring point of discussion,[20] and the HLG broadly agreed that a mechanism or scheme to ensure that such tools comply with the accountability and forensic standards within the Union was warranted. Evaluation and certification are needed to guarantee that technologies meet trustworthiness requirements (e.g. requirements on data integrity throughout the digital forensic process), regardless of whether the manufacturer is established inside or outside the EU.

17 https://enfsi.eu/
18 See Recommendation 1
19 See Recommendation 3 and 4
20 See Recommendation 5

Among the problems identified by the HLG was also a **decrease in communication** between law enforcement and the providers and suppliers of hardware and software; as a result, law enforcement authorities encounter difficulties as how to engage with industry to be granted access to data on seized devices. The HLG found that a lack of knowledge affects interactions that law enforcement authorities have with producers of hardware and software. The decreasing communication between law enforcement and industry also led to the establishment of fewer protocols for lawful access to data on users' devices. The HLG set out that the lack of law enforcement's participation in the standardisation bodies affects the possibility to shape product protocols and technical architecture in such a way to ensure that their concerns and technical requirements are taken into account at an early stage in the development of future technological standards.[21]

A final key issue addressed by the HLG was that, in the absence of voluntary cooperation, a **lack of obligations for industry** to cooperate with law enforcement requests for data at rest in a user's device is negatively affecting their capacity to conduct thorough investigations. They ascertained that there is a lack of any comprehensive overview of existing obligations at the Member State level.[22]

As regards **access to data at rest in a service provider's system**, the first key issue that law enforcement authorities confront revolves around discrepancies among domestic legal frameworks regulating the retention of data within providers' systems and the duration of such retention.

Experts highlighted notably the current absence of any level of **harmonisation of data retention legislation** across the EU and difficulties in meeting the criteria indicated by the CJEU, limiting general and indiscriminate retention of traffic and location data under specific circumstances to fighting serious security threats and allowing only targeted retention of such data for fighting serious crime. In particular, the concept of targeted data retention is proving very difficult for Member States to implement, in part also because some of the criteria were designed based on technologies that have evolved since the judgments were issued,[23] and a lack of clarity concerning what types of data can be accessed for non-serious offences persists.

[21] See Recommendation 12

[22] See Recommendation 25

[23] For example, technologies like dynamic IP addresses and Carrier Grade Net Address Translation (CGNAT) were not fully developed at the time of publication of the CJEU judgements which suggested data retention based on geographic targeting (see for reference cases Digital Rights Ireland, 2014 and Tele2 Sverige AB, 2016).

The HLG held a harmonised approach to data retention at EU level to be indispensable for effective investigations, in particular in cross-border cases, and for admissibility of evidence in courts. They also discussed how the absence of data retention obligations can affect the effectiveness of the new e-evidence rules, as traffic data subject to European preservation or production orders might be unavailable.

The HLG shared the view that any solution to the current challenges needs to be technology-neutral, in order to cover any future technical developments. Emphasis was put on the need for such solutions to create obligations for all service providers, including OTTs, who should be compelled to reply to requests from LEAs and be more transparent with regard to the data that they collect for business purposes. Such a regime could be achieved through **legislation or soft law measures**, with a preference for the former.[24]

In light of the jurisprudence on data retention, the HLG discussed the practical application of **targeted retention** and stressed the difficulties encountered in the implementation of the requirements of the Court, (i.e. targeting retention based on geographic criteria and categories of persons). Implementing the Court's requirements was considered problematic by the experts with respect to fundamental rights (because of discrimination against categories of persons or location), from an operational point of view, as targeting the collection of data drastically reduces the capacity to access vital information for investigations, and from a technical implementation perspective for the operators. In light of these considerations, many experts stated that an EU regime should focus not only on retention, but also on access. In particular, some experts expressed the opinion that differentiating the time limits to access retained data on the basis of categories of crime should be the only criterion regulating data retention regimes, and that solutions for very targeted access be designed on the basis of other criteria.[25] However, some other experts raised concerns how these measures would comply with the CJEU jurisprudence, as the CJEU case-law applies to both data retention and data access.

[24] See Recommendation 27
[25] See Recommendation 29

Among the problems identified, law enforcement authorities also face difficulties relating to the **types of metadata retained** by service providers. Where legal obligations exist, they at times leave flexibility to communications service providers as regards the types of metadata that should be retained; this results in a variety of available data with different degrees of usefulness as investigative leads. The HLG took the view that the EU should require minimum levels of retention (at least of data needed to identify a user) from operators, would need to be imposed on operators at EU level.[26] The HLG also agreed that service providers offering encrypted services must be obliged to find the means to provide data in an intelligible way upon lawful request from law enforcement and judicial authorities.[27]

The shift from traditional communication providers towards the use of **OTTs** is a key driver of the difficulties that law enforcement face when attempting to access data stored on service providers' systems. While OTTs fall within the scope of the European Electronic Communications Code (EECC), they are not subject to comparable licensing systems that can potentially entail obligations. Experts discussed the compelling need of rules obliging OTTs to retain data also in the case that they are based in different jurisdictions. The lack of such rules results in a lack of clarity and legal certainty, leading to, non-compliance from their side. Additionally, certain OTTs sometimes retain no data at all.

The HLG agreed on the need for **transparency** on data generated, processed, and stored by communication providers, including in particular OTTs and other services that offer "communication services" (like car manufacturers)[28] and discussed instruments to enforce compliance prior to entering into operation in the EU market.[29] Experts discussed the opportunity to legislate on data already in the possession of providers for business purposes.[30]

[26] See Recommendation 27.v
[27] See Recommendation 27.iii
[28] See Recommendation 17
[29] See Recommendation 30
[30] See Recommendation 31

In this context, experts agreed on the need to establish **cooperation mechanisms** with the private sector aimed at increasing transparency, and suggested several possibilities to do so, including by means of Memoranda of Understanding[31] and by reinforcing and fully exploiting existing structures such as SIRIUS, EJN[32], and/or the EJCN.[33]

The HLG saw value in enhanced cooperation, also when it comes to defining standardised formats for data retention.[34] In fact, while a standard developed under the auspices of the European Telecommunications Standards Institute (ETSI) exists for traditional telecommunications metadata, it is not universally applied across the Member States even with telecommunications providers, and there is no agreement on a standardised format for data transmissions from OTTs to law enforcement authorities. This adds complexity to the data analysis in cases where data can be provided at all.

S**tandardisation** should be pursued to ensure harmonised categorisation of data to be retained and accessed, but also for establishing secure channels for the exchange between competent authorities and service providers. The HLG discussed several possibilities to do so, focussing in particular on enhancing a coordinated participation of law enforcement representatives in relevant standardisation bodies.[35]

Most Member States have dedicated national regulatory frameworks in place for **real time access to communication data**, which remains an essential tool for the fight against crime, including online crime and organised crime as well as terrorism.

However, when it comes to non-traditional service providers, law enforcement authorities cannot rely upon an enforceable and harmonised framework. In fact, while some Member States have established regulations which oblige OTTs to respond to lawful requests for such access, there is an **uneven implementation** between communication service providers (CSP) and OTTs on real time access to data, with OTTs generally not implementing such obligations owing to legal and technical reason.

---

31 See Recommendation 14

32 The European Judicial Network in criminal matters (EJN) is a Network of national Contact Points for the facilitation of judicial cooperation in criminal matters.

33 See Recommendation 13

34 See Recommendation 15 and 16

35 See Recommendation 20

The experts agreed that one of the main objectives would be to **create a level playing field between CSPs[36] and other types of electronic communication providers** when it comes to enforceable lawful interception (LI) obligations; lawful interception must be provided for in law and authorised by courts or independent administrative authorities in line with technical standards and in full compliance with data protection and privacy, as well as cybersecurity and interoperability measures. Experts clarified in many instances that lawful interception of electronic communications services should be the preferred measure to access data in real time. Such lawful interception rules should be based on principles that currently apply to traditional communication providers, for example in terms of oversight and cooperation with operators of communications, but also in terms of ability to access data in clear when deemed necessary and proportionate by judicial authorities.[37]

Differences in the domestic legal frameworks of EU Member States on interception of metadata or content data create challenges for law enforcement in cases with cross-border elements. For instance, it may be difficult for law enforcement authorities to intercept in real-time communications between two citizens in their country who use a communication service hosted in another EU Member State with different procedural requirements for live interception. Experts discussed the opportunity to solve these issues at EU level, detailing different measures that could be implemented to this purpose, e.g. legislative actions.[38] The legal uncertainty stemming from different requirements across national legal frameworks concerning interception was a central topic of discussion among the experts, who elaborated on the need to address issues such as the territorial application of certain obligations, which results in conflicts of law and delays or administrative obstacles to investigations.[39]

In addition to the issues determined by the lack of harmonised legislation across Member States, experts also discussed the fact that **the lack of knowledge of the precise location of users and data often adds complexity to determining the territorial nexus of a criminal offense**.

[36] Traditional telecommunication providers under ETSI definition i.e. infrastructure owners
[37] See Recommendation 37
[38] See Recommendation 38
[39] See Recommendation 39

While experts agreed on further exploiting the European Investigation Order (EIO) as a tool for requesting interception by another Member State and for the exchange of evidence collected through interception, they also discussed its limits, including those related to the partial applicability across Member States.[40]

The concept of territorial jurisdiction over data was raised during the discussions. Experts considered that in cases where the nexus is national (e.g. a crime committed in one Member State by a criminal located in the same Member State), a state's authority should be able to adopt interception measures, in accordance with national procedural law setting out requirements and safeguards, without going through a cross-border cooperation instrument. Where necessary to overcome conflicts of law with other jurisdictions, the experts discussed possible initiatives that the EU could take, drawing inspiration from the e-Evidence Regulation, and consisting also of bilateral agreements with countries such as the United States, supported by further analysis, and an impact assessment that considers also fundamental rights and state sovereignty, the experts discussed.

Experts shared the view that some level of harmonisation at EU level could be sought through soft law (e.g. a Commission Recommendation), while they suggested that common operational needs of LI could be developed on the basis of the LEON document.[41]

From a technical perspective, experts discussed **the need to set up mechanisms and infrastructures that are compatible with the transfer in real time of interception of potentially very large amounts of data of various nature**.[42] In relation to this, experts discussed at length the benefits of standardisation and possible approaches in that domain. They called for a stronger representation of national government/administration in the development of standards for 5G/6G and communication in general, insisting on the need of being present in the most relevant forums such as 3GPP, ETSI, ISO and ITU. Support from the Commission, Europol or other EU bodies or agencies was also considered necessary.[43]

[40] See Recommendation 40
[41] See Recommendation 21
[42] See Recommendation 9
[43] See Recommendation 20

In parallel, experts discussed in depth the cases relating to non-cooperative providers so as to be able to sanction them as appropriate, with administrative and/or criminal sanctions, depending on the level of negligence.[44] Experts were in agreement that any future EU instrument in this regard should take into account this difference.[45] It should also take into account the EU acquis, notably the Digital Services Act.

For cases of non-cooperative providers, experts discussed and shared the view that, regardless of the legal instruments in place, in **specific cases** (e.g. primarily criminal services, such as EncroChat), **law enforcement authorities will still need to resort to the use of vulnerabilities** (i.e. intrusive measures). While there was consensus that those cases should remain exceptional and such solutions are far from being ideal, it is important to cooperate on harmonisation of these aspects, especially in consideration of establishing safeguards[46] and -possibly- harmonised rules for the mutual admissibility of evidence between Member States to the extent necessary to facilitate mutual recognition of judgments, judicial decisions and police and judicial cooperation in criminal matters.[47] Experts stressed how operations such as EncroChat or Sky ECC are challenged in courts, and highlighted the legal uncertainty that results from the different requirements across national legislations when it comes to the use of an outcome of an intercept in one Member State as evidence in another.

Another issue identified as a problem and extensively discussed pertains to **access to data in readable format.**

In addition to the problems on accessing data on the device, encryption adds a level of complexity when it comes to accessing real time content data, both for OTTs when implementing an end-to-end encryption mechanism, and for traditional telecommunication operators when, for example, implementing "Home Routing" for 5G.

---

44 See Recommendations 33
45 See Recommendation 34
46 See Recommendation 10
47 See Recommendation 42

On **accessing content data despite encryption**, experts extensively discussed and agreed upon the need for law enforcement to have access to data *en clair*. They stressed that technological solutions can be implemented where they exist or should be developed to preserve privacy and data protection, guarantee cybersecurity, and enable the implementation of targeted lawful access measures at the same time, including on content data. Experts discussed the need for standardisation to address law enforcement's operational requirements, notably in new telecommunication standards such as 6G. Standards that enable lawful access without weakening privacy, data protection, and cybersecurity mechanisms[48] should be developed for present and future communication technologies. This approach, that shall involve the evaluation and certification of lawful interception systems to guarantee that cybersecurity, privacy, and lawful access requirements are actually met, opens a perspective in the longer term and for upcoming technologies such as 6G.

Experts expressed the wish **to first explore technical aspects,** in coordination with cybersecurity experts. They clarified the need to address the challenges of encryption (and of real time interception more globally) as **from the design of communication technology**, notably by **developing projects involving technology, cybersecurity, privacy, standardisation and security experts.** They stressed that, to perform their duties in the digital world, law enforcement authorities need to have a pre-established lawful access to readable data, in accordance with international instruments such as the Budapest Convention, and while preserving cybersecurity requirements. To that aim, the HLG called for the EU to set up a roadmap and coordinate the work through a permanent structure process, possibly hosted by the EU Innovation Hub for Internal Security.[49]

Related to the above, further elements of concern included the use of rich communication services (RCS) to exchange SMS' in an end-to-end encrypted manner and the increased 5G communication for inbound roamers and initiatives such as Apple Private Relay. Technologies like these cut traditional telecommunications service providers from the most relevant information, otherwise available in clear, thus impacting the ability of law enforcement to access real time data in transit effectively and lawfully. Experts debated these challenges and stressed the need to maintain lawful interception capabilities for traditional telecommunication operators despite 5G and 6G and called for cooperation with service providers to be facilitated at EU level.[50]

[48] See Recommendation 23
[49] See Recommendation 22
[50] See Recommendation 24

Recommendations of the High-Level Group

With regard to Capacity Building measures, the High-Level Group recommends:

1. Mapping and connecting **existing digital forensic networks** while increasing accessibility, avoiding overlaps, and fostering leadership. Regarding the latter, a secretariat for the networks should be established, to simplify the dissemination of knowledge among experts; the secretariat should reflect on mechanisms to ensure that sensitive tools can be shared in full respect of national rules.
2. To reflect on **mechanisms for pooling knowledge**, to ensure that digital forensics tools can be shared between Member States in an environment of trust, whilst taking into account national rules. This could include exploring a European approach for the management and disclosure of vulnerabilities handled by law enforcement, based on existing good practices.
3. The development of a mechanism at EU level for **jointly purchasing the licenses of digital forensic tools**, to share them among Member States.
4. Increasing **funding for research and development of tools for data acquisition, access to data in clear including decryption capabilities, and artificial intelligence-based capacities for data analysis** with clear deliverables, and promoting the Europol Tool Repository as a central hub for the dissemination of these tools.
5. Creating a **mechanism/scheme for the evaluation and -when relevant- for the certification of commercial digital forensics tools** at EU level, being mindful of any potentially negative impact on the investigation and prosecution processes (such as adding unnecessary burden).
6. Setting up a process dedicated to the **exchange of capacities** that potentially imply the use of vulnerabilities, which would allow the pooling of knowledge and of resources, whilst respecting the confidentiality and sensitivity of the information.

7. Increasing the number of **training opportunities** for experts and creating a **certification scheme at the EU level for digital forensic experts** (including for those working on decryption), to guarantee the quality and uniformity of technical training provided.

8. Investing to fill the gap in technical skills in standardisation and increasing awareness by establishing **agreements with academia** and other relevant institutes.

9. Building **mechanisms (interoperability and cybersecurity) and infrastructures (bandwidth and scalability) that are compatible with the transfer in real time of large datasets**, such as those collected when authorities in one Member State execute a lawful access request on behalf of another Member State. This implies further work on the standardisation of data structures, on trust mechanisms, and on data filtering, to avoid the transmission of data not relevant for investigation(s) and meet the data protection principles of purpose limitation, proportionality, and data minimization, together with work conducted at EU level on the design and dimensioning of means of transmissions and the associated costs.

10. Working in a more coordinated manner and with the support of EU funding on a **methodology to develop, handle, and use targeted lawful access measures** to address cases where access to data is not possible through cooperation with Electronic Communications Services. Considering its sensitivity, such approach should be subject to judicial authorisation and with a sound framework on the admissibility of evidence. Those cases should remain exceptional – i.e. law enforcement authorities should only make use of such tools as a measure of last resort - and be subject to mandatory proportionality assessments.

With regard to Cooperation with Industry and Standardisation, the High-Level Group recommends:

11. The creation of a **platform (equivalent to SIRIUS[51])** to share tools, best practices, and knowledge on how to be granted access to data from product owners and producers. Building further on SIRIUS, **t**his should be expanded to include hardware manufacturers in its mandate and to create and map law enforcement points of contact with digital hardware and software manufacturers.

12. Fostering **cooperation with producers and developers of digital forensic tools** to streamline the structure and format of data obtained by law enforcement authorities through the use of those tools, ideally following agreed standards.

13. Further funding, expanding, and **establishing permanently EU structures** and forums, including SIRIUS, EJN and/or EJCN, for the purpose of: (a) developing contacts between practitioners and service providers to support exchange of information, capacity building and training, (b) nurturing a permanent dialogue, including through a forum or an independent authority that brings together practitioners (LEAs, judiciary and service providers), to define the principles and modalities for cooperation. This could include creating or supporting a **central repository of tools and information** (CRIP) allowing for sharing jurisprudence, changes in legislation and other information that would be relevant to Member States and service providers.

---

51 SIRIUS is an EU-funded project that helps law enforcement and judicial authorities access cross-border electronic evidence in the context of criminal investigations and proceedings. Co-implemented by Europol and Eurojust, in close partnership with the European Judicial Network, the SIRIUS project is a central reference point in the EU for knowledge sharing on cross-border access to electronic evidence. The SIRIUS project helps investigators cope with both the complexity and volume of information in a rapidly changing online environment. The project provides products such as standardised guidelines on cooperation processes between competent authorities and specific service providers (SPs). Other services SIRIUS provides includes investigative tools and contact details for SPs, and SIRIUS also facilitates opportunities to share experiences with peers, both online and in person.

14. The adoption by Member States of **Memoranda of Understanding** as an effective mechanism to promote co-operation and develop a common understanding between service providers, government, and law enforcement agencies to support the operation of national laws, making use of best practices established in certain Member States.

15. The development of data formats following the **standards developed by the European Telecommunications Standards Institute (ETSI)** or other standardisation bodies to foster interoperability and facilitate exploitation by all Member States.

16. Progressively replacing specific formats used by each service provider (and consequently Member States' authorities) with a horizontal approach, based on standards developed by ETSI or by other standardisation bodies for the format of requests and replies. *[The coherence of this recommendation with the rules established by the e-evidence Regulation should be further assessed]*

17. **Fostering transparency rules for providers of Electronic Communications Services** with regard to the data that they process, generate or store (as these do not always coincide) in the course of business, and on informing law enforcement authorities about what data is available, taking into account limits posed by the confidentiality of investigations. Experts suggest achieving that goal through cooperation agreement with service providers or, if necessary, by setting mandatory obligations. Increased transparency is also needed in the implementation of lawful interception obligations for judicial purposes, both from the side of Electronic Communications Services and from the side of authorities. Such rules should go hand in hand with the notion of the secrecy of the investigation. For example, in all investigations it is imperative that suspects are not notified for the whole duration of the investigation.

18. Creating a **clearing house** to identify the relevant service provider(s) and target lawful requests to them (e.g. for number portability for telecommunications providers, as already exists in some EU Member States).

19. Establishing mechanisms to ensure that cross border requests are targeted to service providers in a manner that is efficient and avoids potential conflicts, taking inspiration from mechanisms set for e-evidence. *[the coherence of this recommendation with the rules established by the e-evidence Regulation should be further assessed]*

20. Accompanying future initiatives with relevant **standardisation measures**. To that aim, it is suggested that the Commission puts forward a **roadmap**, including a long-term perspective defining clear objectives, foreseeing adequate funding to support an increased participation of Member State experts and proposing a coordination mechanism, possibly through Europol and other EU agencies. It should be ensured that the scope of standardisation activities is broad and encompasses the internet of things, including, for example, connected cars as well as any forms of connectivity including for example satellite communications. Activities related to digital forensics, lawful access, and lawful interception should be covered.

21. Drawing inspiration for future legislative, practical, and technical initiatives from a **common definition of requirements**, such as set out in **LEON (Law enforcement Operational Needs for Lawful Access to Communication[52])**. The set-up of an ad-hoc group of experts, possibly coordinated by Europol, would ensure that LEON is updated where needed, possibly under the coordination of the working group on standardisation for security hosted by Europol that should be continued. Any initiative should be technology neutral. Different options can be envisaged to refer to LEON in future EU initiatives: (1) EU legislative proposal that would make a reference to LEON, (2) recommendation, (3) source of inspiration.

---

52 LEON is the outcome of work undertaken by Swedish law enforcement agencies, in close co-operation with law enforcement representatives in EU Member States, North America and Australia. The aim is to identify and describe the law enforcement needs for lawful access to communications content, content related data and subscriber information.

22. Developing a technology roadmap that brings together technology, cybersecurity, privacy, standardisation and security experts and ensures adequate coordination e.g. potentially through a permanent structure, in order to implement **lawful access by design** in all relevant technologies in line with the needs expressed by law enforcement, ensuring at the same time strong security and cybersecurity and providing for the full respect of legal obligations on lawful access. According to the HLG, law enforcement authorities should contribute to the definition of requirements, but it should not be their role to impose specific solutions on companies so that they can provide lawful access to data for criminal investigative purposes without compromising security.

23. Ensuring that possible new obligations, a new legal instrument and/or standards **do not lead, directly or indirectly, to obligations for the providers to weaken the security of communications** by generally undermining or weakening E2EE. Therefore, potential new rules on access to data in clear would need to undergo a cautious assessment based on state-of-the-art technological solutions (which should in turn consider the challenges of encryption). When ensuring the possibility of lawful access by design as provided by law, manufacturers or service providers should do so in a way that it has no negative impact on the security posture of their hardware or software architectures.

24. Enhancing **EU coordination and support** to address situations where technical solutions exist to enable lawful interception but are not implemented by providers of Electronic Communications Services. In such cases, for example when home-routing agreements or when specific implementation of Rich Communication System (RCS) do not allow lawful interception capabilities, clear guidance and a dialogue facilitated at EU level would improve the cooperation with Electronic Communications Services.

With regard to Legislative measures, the High-Level Group recommends:

25. Conducting a **comprehensive mapping** of the current legislation in Member States to detail the legal responsibilities of digital hardware and software manufacturers to comply with data requests from law enforcement. It would also take into account specific scenarios and requirements that compel companies to access devices, in compliance also with CJEU case-law and case law of the European Court of Human Rights. The goal should be to develop an **EU-level handbook** on that basis, and depending on the aforementioned mapping, to promote the approximation of legislation within this area, and to develop binding industry standards for devices brought to market in the EU, to integrate lawful access.

26. Establishing a **research group to assess the technical feasibility of built-in lawful access obligations** (including for accessing encrypted data) for digital devices, while maintaining and without compromising the security of devices and the privacy of information for all users as well as without weakening or undermining the security of communications.

27. Establishing a **harmonised EU regime on data retention** with the following features:

    i. be technology neutral and future-proof,

    ii. covering present and future "data handlers" (i.e. OTTs and service providers of any kind that could provide access to electronic evidence),

    iii. ensure access to intelligible data (for metadata and subscriber data, there should be a means for the service provider to decrypt the data if encrypted at any time during the provision of the service),

    iv. not only focus on data retention, but also on access to data, building upon the e-evidence rules,

    v. establish at the very least an obligation for companies to retain data sufficient to ensure that any user can be clearly identified (e.g. IP address and port number),

    vi. in full compliance with data protection and privacy rules.

28. **Categorising** data on the basis of its purpose (identifying, locating, establishing the online activity of a subject of interest), although some work is needed to translate the purposes into clear technical requirements.

29. **Ensuring that access to data is targeted and differentiated** depending on data categories or on specific categories of crime (e.g. crimes that only happen on the Internet) or on the basis of the threat to victims.

30. **Including rules on accountability and enforceability** for service providers in order to enforce obligations to retain and provide data, e.g. through the implementation of administrative sanctions or limits to operate in the EU market.

31. **Making sure that user data retained for commercial and business purposes** is effectively accessible for law enforcement under relevant safeguards.

32. Considering setting **obligations on service providers** to turn on or turn off certain functions in their services to obtain certain information after receiving a warrant (for example storing geolocation of a specific user after s/he is targeted by a lawful request).

33. Developing a mechanism to ensure that Member States can **enforce sanctions** against **non-cooperative Electronic Communications Services**[53], and that such measures act as a deterrent against those entities. Both administrative and criminal law measures should be available and should be applied depending on whether a provider is merely non-cooperative or is deliberately hosting activities of a criminal nature.

34. Harmonising at EU level criminal law measures to enforce cooperation, including imprisonment. The same should apply to **non-cooperative hosting providers** (in addition to Electronic Communications Services) to ensure that such companies, when hosting communication services of a criminal nature, adequately comply with the judicial orders they receive. *[The coherence of this recommendation with the rules established by the Digital Services Act Regulation should be further assessed]*

[53] In that context, **Non-cooperative Electronic Communications Services** is defined as any operator who does not comply with legal orders and requests of a technical nature addressed by the law enforcement and has no objective reason for doing so.

35. Potential initiatives should distinguish between **criminal Electronic Communications Services** providers (i.e. platforms that are specifically designed to offer services solely or mainly to criminal actors, such as EncroChat) and **non-cooperative Electronic Communications Services**, which are legally established and conduct lawful activities but do not fully comply with national obligations on lawful interception.

36. Establishing an **enforceable obligation for platforms** (or alternatively soft measures through cooperation with industry) to designate a **SPOC[54] (Single Point of Contact)** in the EU for handling of requests from and contacts with EU authorities, especially for service providers for which an emergency contact is needed. A similar mechanism (or ideally the same SPOC, with extended prerogatives) should also exist to facilitate **the enforcement of obligations on lawful interception**.

37. Subjecting providers of Electronic Communications Services (ECS) (as defined in the European Electronic Communication Code - EECC[55]) to the same rules as traditional service providers.

38. Further **harmonising national legal frameworks for access to data in transit[56]** through several steps:

    i. Ensure that lawful interception obligations set out in national laws are **enforceable on a broader range of communication providers**, including relevant categories of internet service providers (and seek inspiration in that respect from the e-evidence package).

    ii. Seek harmonisation at the EU Member States level on the basis of **agreed common principles** (notably those part of the LEON document – Law Enforcement Operational Needs) through soft law (e.g. a Commission Recommendation).

[54] SIRIUS initiative created in 2020 the SIRIUS SPoC Network with a dedicated platform on the Europol Platform for Experts. It is currently composed of 39 LEAs from 22 EU countries and 2 third countries.

[55] Article 2, point (4), of Directive (EU) 2018/1972

[56] The notion of data in transit may cover cases where data acquisition is not performed while being in transit but when communication data is about to be sent or has been received (sometimes defined as "live data").

iii. Reflect on a **definition of lawful interception** in the broad context of internet communication services, also distinguishing between lawful interception of non-content and of content data.

iv. Based on further analysis and an impact assessment, including from the perspective of fundamental rights and taking into account the sovereignty of States in criminal matters possibly put forward an EU initiative on lawful interception (consisting of soft law or legal instruments) taking inspiration from the work done under e-evidence and working on international and bilateral agreements (e.g. with the United States). Such initiative would need to ensure that "lawful access by design" principles are properly implemented by relevant stakeholders (e.g. ECS) to meet defined requirements, notably to enable access data in clear when deemed necessary and proportionate

39. Adjusting the **concept of territorial jurisdiction over data** to address potential conflicts of laws with other jurisdictions. In cases where the nexus is national (e.g. a crime committed in one Member State by a criminal located in the same Member State), it should be possible to set up an interception measure, in the framework of national procedural law setting out requirements and safeguards, without going through a cross-border cooperation instrument.

40. Exploring how the **European Investigation Order (EIO)** could better support efficient cross-border lawful interception requests by improving legal certainty, shortening delays for responding to warrants, and fostering a uniform usage of the EIO and the Council of Europe "Budapest" Convention on Cybercrime throughout Europe to close existing gaps on access to data.

41. Reflecting on **necessary safeguards** when lawful interception applies to non-traditional communication service providers. Some experts suggest that this investigative measure should only concern communications that are taking place after the reception of a legal request from the authorities. In addition, measures should not imply an obligation for providers to adjust their ICT systems in a way that negatively impacts the cybersecurity of their users.

42. Adopting minimum rules at EU level allowing for the mutual admissibility between Member States of **evidence** obtained from lawful interception measures against non-cooperative providers and providing for the admissibility also in case of use of intrusive measures, to the extent necessary to facilitate mutual recognition of judgments, judicial decisions and police and judicial cooperation in criminal matters.