10 August 2025

Public consultation on "retention of data by service providers for criminal proceedings"

Answering guide for civil society organisations and individuals

The European Commission has launched a public consultation to gather your views about the impact of data retention rules in view of adoption of legislative and non-legislative measures at EU level.

In her political guidelines, the President of the Commission, Ursula von der Leyen, has announced that she wants "to provide law enforcement with adequate and up-to-date tools for lawful access to digital information, while safeguarding fundamental rights". More specifically, in her mission letter to the candidate for the Home Affairs portfolio, Magnus Brunner, she indicated two objectives:

- (1) an 'update' of law enforcement's tools for access to digital data and
- (2) 'rules on data retention'.

What is "data retention"?

In the context of this consultation, data retention is a requirement obliging providers of electronic communications services (email, private messaging, internet access providers like telecom companies, etc.) - we call them 'service providers' (SPs) - to retain certain types of data related to their users beyond what is necessary for the provision of their services and only for law enforcement purposes.

What data is concerned?

Mainly traffic and location data. Traffic data is metadata about your online activities. Whenever a device accesses a communications network, small packets of data related to that device's

activities are processed on the systems of the operator responsible for the network.

This includes all other information about a communication other than the communications content, such as the communication's origin (who sent it?), the destination (who is the recipient?), the route, the time, the date, the size (of the message), the duration (of the activity), or the type of underlying service.

Metadata can be compared to the information outside an envelope (address, weight, format, stamps, etc.); the communications content corresponds to the message inside the envelope.

It is possible to learn A LOT about an individual's movements, interests and social network from analysing metadata - even without ever accessing the actual content of their communications. It is well established that metadata can reveal information that is no less sensitive than the actual contents of communications.

Read more:

- How much does location data reveals: https://interaktiv.br.de/ausspioniert-mit-standortdaten/en/index.html
- How much does metadata reveals: https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

Wasn't this already a thing of the past?

Yes, in theory. In 2014, the Court of Justice of the European Union (CJEU) invalidated the old EU Data Retention Directive because it required a mass and indiscriminate retention of all traffic and location data, which was considered in violation of the Charter of Fundamental Rights. Unfortunately, since then, the vast majority of Member States have ignored the CJEU ruling(s) and maintained illegal national data retention laws.

This legislative proposal has the potential to legalise (again) mass surveillance at the European Union level and to undermine online privacy and other fundamental rights depending on it (freedom of assembly and association, of expression, etc.). Moreover it creates very serious cybersecurity risks as all the data retained is vulnerable to (increasing) cyberattacks.

For more information about data retention and the state of play, please see EDRi's response to the Commission's call for evidence.

This is why your contribution in this consultation process is **extremely valuable** to speak up against the surveillance agenda of the Commission and law enforcement authorities.

We have prepared this guide:

- to help you navigate within this consultation, and
- to suggest answers to the questions based on upholding human rights.

Most questions are multiple choice questions and only a few have short free-text boxes.

GETTING STARTED

Go to the consultation page and click on "respond to the questionnaire" – you will first be asked to create an account for the EU survey portal if you do not already have one. Once registered, you will be asked to identify yourself, the capacity in which you are answering the consultation (NGO, EU citizen or non-EU citizen (sigh)), your country of origin and email address, all of which are **mandatory**.

The Commission is unlikely to contact you using this data, except to confirm your response. It also informs you that it will make your answer public – you can choose to have **your name included or remain anonymous** when your contribution is published. Your email address will never be published.

HOW TO NAVIGATE THE CONSULTATION

At the top of the page, you will notice that the consultation is divided into 3 main sections – it is very short. You have the possibility to submit an attachment to complement your feedback at the end.

GENERAL QUESTIONS ON THE NEED FOR AN INITIATIVE

1. How are you affected by legislation in this area?

Here you are asked again to specify in which capacity you are concerned by the subject matter. The Commission seeks to have a more detailed overview of the respondent categories interested in data retention. You may therefore choose the category that reflects best your situation (user, lawyer, employee of an NGO, academic or other).

2. Do you consider that, in today's digital society, public authorities in charge of investigating

and prosecuting crimes have sufficient tools at their disposal?

We recommend to select "Fully agree".

The Commission seeks to legitimise its initiative by obtaining public support to the idea that law enforcement struggles to carry out their work in the digital age because they cannot access digital data. However,

- **this assumption is not backed up by any reliable evidence**: despite countless requests by EDRi, academics and other civil society actors for proof that mandatory data retention is necessary, the Commission and Member States' law enforcement authorities have constantly failed to provide reliable evidence about the marginal benefits of indiscriminate retention of electronic data compared to less intrusive alternatives. The preferred tactic of the Commission is to use anecdotal evidence, for example news coverage about a specific police investigation where access to retained data had been useful, to justify new data retention initiatives. This leads to legislative proposals (for general and indiscriminate data retention) which do not satisfy the necessity test.

- with the pervasive use of online services and smartphones, and the predominant business model of surveillance capitalism which leads to massive data collection for commercial purposes (e.g. behavioural advertising and training large AI models), **law enforcement is literally enjoying** a golden age of surveillance **with access to more data about European residents than ever before**. Mobile phones have become ubiquitous and enable law enforcement to track the physical movement, social networks, preferences and habits of everyone.

3. In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, because of a lack of available digital evidence which can enable, among other things, the identification and localisation of suspects. To what extent do you agree with this statement?

We recommend to select "Fully disagree".

Same as above.

To the contrary, analysis of **large volumes of data already available to investigators has actually become a problem.** That's not us saying it, it's EU agencies for law enforcement and judicial cooperation, Europol and Eurojust (see pages 6-7). Law enforcement is now requesting AI tools to sift through the large amounts of data they collect (often unlawfully) because they can no longer

do so manually. It is therefore not the lack of data, but, in many cases, the lack of technical capacity to analyse vast quantities of already available digital data that (supposedly) hinders criminal investigations.

4. In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, due to lack of of legal obligations or rules. To what extent do you agree with this statement

We recommend to select "Fully disagree".

Law enforcement authorities have multiple legal instruments to access digital information:

- in domestic cases, they rely on national laws to send data access requests to services providers under their jurisdiction. All Member States do have rules in place regulating the data production process for law enforcement processes.

- in cross-border cases (when the service provider is located outside of their national jurisdiction), authorities may rely on several tools depending on the case:

    - Mutual Legal Assistance Treaties (MLATs)

    - the European Investigation Order (EIO)

    - from August 2026: the 'e-Evidence' Regulation.

5. In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, due to lack of human resources, skills, training, etc. To what extent do you agree with this statement

We recommend to select the answer you deem the most appropriate. "I don't know" is a valid answer.

We don't have enough information to evaluate law enforcement's capacities to efficiently conduct investigations and prosecutions.

It is true, however, that internet companies often report how law enforcement's requests for data are sometimes erroneous (e.g. ask for data that they don't process), reflect a lack of technical understanding or are sent with low and poor cybersecurity protections (e.g. unencrypted, by fax, etc.).

Furthermore, we know that in cross-border cases, **one of the main issues is the lack of resources allocated to the judicial review of requests** for data by foreign authorities. In the context of MLATs (see question above), investigative authorities complain that it takes too much time for their requests to be processed to the extent that once they are, it is too late and the data has been deleted already. But that's mainly because of a lack of human resources. In 2019, thanks to the "MLAT Reform" program, the U.S. Department of Justice reduced the amount of pending cases by a third.

6. How familiar are you with laws and policies related to retention of metadata by service providers for the purpose of preventing, detecting, investigating and prosecuting crimes?

The answer is up to you, but we can give you some background information to help you decide. First of all, **you don't need to be an expert on data retention in order to respond to the consultation, because data retention affects all of us.**

Currently, there is no EU-wide law on mandatory data retention. However, most Member States have national laws on data retention that originally implemented the Data Retention Directive from 2006, which was declared invalid by the CJEU in 2014. In some Member States, amendments to these laws have been made in an attempt to comply with data retention rulings from the CJEU.

The question is not about detailed knowledge of all of these national laws (very few people have that!), but rather knowledge about the subject of mandatory data retention. Since you are responding to the consultation, you are probably aware of the existence of such rules and policies, but you may not know the details. If you have studied data retention more closely (e.g. following news coverage or reading blog posts from digital rights organisations such as EDRi), you can consider responding 'detailed knowledge of the subject' - if you feel comfortable about that. You don't need to know everything about which metadata is retained and for how long in order to have detailed knowledge of the subject. Your detailed knowledge of the subject can also be about Member States refusing to comply with the data retention rulings from the CJEU.

Service providers store, for limited periods, certain metadata (such as subscribers' data, IP addresses and other communication data that do not concern the content of any communication) that they generate, process and store, for legitimate business purposes.

7. Do you consider that, to ensure criminal justice, service providers should retain metadata for longer periods, or that they should retain additional types of metadata that could be relevant for investigations and/or prosecutions, for the specific purpose of law enforcement?

We recommend to select "No, providers should be allowed to retain data exclusively for business purposes and no longer. Law enforcement should rely only on such data."

As explained above, firstly, mandatory data retention for law enforcement purposes **was never proven to be necessary** and **other less intrusive alternatives**, such as relying on expedited targeted preservation of stored data, **were never demonstrated to be less efficient** to achieve the same goals. Most law enforcement requests for non-content are actually successful, even in Member States without a data retention law. According to a 2020 Commission study, only slight variations can be detected between LEA (law enforcement authority) survey respondents from Member States with and without mandatory data retention. The retention periods for non-content data are invariably shorter in Member States without mandatory data retention, but **the German police have managed to adapt to the shorter retention periods by obtaining judicial approval for access requests within a week**. There are also no discernible differences in terms of crime clearance rates between Member States without mandatory data retention (currently Slovenia, Austria, The Netherlands and Germany) and those with.

Secondly, there is enough (and way too much) personal data collected and processed for commercial purposes about everyone due to the current **dominant surveillance-advertising business model** of internet services.

There is no scientifically sound evidence that the current situation *systematically* prevents law enforcement authorities from carrying out their tasks. Anecdotes are not enough to justify serious interference with fundamental rights, as per the requirements of the Charter of Fundamental Rights.

Thirdly, as we articulated in our submission to the call for evidence, the Court of Justice of the European Union has consistently held that laws requiring general and indiscriminate retention of all traffic data and location data for the purpose of combating (serious) crime are not compatible with EU law.

8. At present, there are no harmonised EU rules obliging or inciting service providers to retain metadata for law enforcement purposes. Do you consider that this brings any challenges?

We recommend to select "No".

The question presumes that harmonised EU rules is the sole solution to current challenges. The Commission lists many of them (when clicking "yes").

However, it is rather the lack of compliance of Member States with *already existing* EU law and the failure of the European Commission to enforce it which are the main reasons for these challenges. In particular to remedy the situation of illegality and to protect Europeans' fundamental rights.

- The predominant explanation for the discrepancies among Member States, is that **most national laws have excessive retention requirements compared to what is permitted by EU law**.
- The CJEU has developed a very detailed case law over the years. **If all Member States amended their national laws to faithfully comply with the requirements set by the CJEU, the challenges noted by the Commission would be considerably reduced.** In particular, legal certainty for service providers and law enforcement authorities as well as safeguards and rights protections.
- When the Commission suggests that "data has already been deleted when it is sought for criminal investigations", it reveals the **real agenda** of reducing discrepancies in Member States' retention requirements: **to increase retention requirements for service providers and thus, surveillance.**

With this question the Commission is trying to make the respondents who have a fundamental rights perspective say that a new EU instrument is the solution to the current rights violations of Member States' national legal frameworks. **Launching infringements procedures against infringing Member States and bringing them back in line with EU privacy requirements should actually be the first action at EU level,** before considering the adoption of new EU rules.

9. Should measures be taken to increase coherence of the data retention rules in the EU for the purpose of investigating and prosecuting crimes?

That's a tricky one. We advise to say "no".

Theoretically and as described above, the measure that should be taken to increase coherence is the launch of infringement procedures against Member States of which data retention laws are contrary to EU law (i.e. the majority of them). However, when clicking "yes", the follow-up questions only propose new (non-)legislative instruments and not enforcement measures. Therefore we recommend to select "no" in order to not legitimise the Commission's future (non-)legislative proposal(s).

10. What do you expect to be achieved by an EU initiative on data retention that cannot be achieved at national level?

- More effective criminal investigations and prosecutions : No – this question is assuming that the indiscriminate retention of traffic and location data of 450 million Europeans de facto leads to more successful investigations and prosecutions which, as stated above, was never demonstrated by facts and statistics (to the contrary).
- Legal certainty for stakeholders involved: No – **It's not guaranteed that an EU initiative actually brings more legal certainty, neither for service providers nor individuals.** The main source of uncertainty is the failure of Member States to revise their national laws and bring them into compliance with the Charter of Fundamental Rights after the Data Retention Directive was struck down by the CJEU. Furthermore, its evaluation in 2011 found that the Directive had created a far larger patchwork of national blanket retention legislation than would have existed without the Directive. It therefore had been counterproductive in achieving its internal market objective of harmonisation. Given Member States' persistent reluctance to harmonise certain aspects of data retention (reimbursement of costs, conditions and procedure for access to and use of the data, purposes for which retained data can be used, any retention requirement that would be lower than their current national one, etc.), it is likely that these problems will persist with a new EU initiative.
- Same obligations for all service providers operating in the EU: No – same as above. It is unclear if Member States would agree on the categories of service providers affected.
- More transparency from service providers about the data they retain: No – this is already addressed by data protection laws (if they were enforced properly but that is a different debate).
- Easier cooperation among Member States: No – **there are already numerous tools for mutual assistance and cooperation at EU level**. The EU should also not constitute a forum for law enforcement authorities to circumvent national constitutional, or otherwise legal, limitations (by relying on another Member State's permissive law to access data).
- Stronger protection of fundamental rights in accordance with the Charter of Fundamental Rights: Yes – **the Commission could enforce the ePrivacy Directive and force Member States to respect the CJEU rulings in order to guarantee the rights to privacy and data protection.**
- Others: Yes

If other, please specify: "Enforcing the requirements laid down by the Court of Justice of the European Union".

11. Which concerns could an EU initiative in the area of data retention raise in your view? Pick the five main concerns

Maximum 5 selection(s)

- [x] Chilling effects on certain fundamental rights, such as freedom of expression.
- [ ] Risk of retention of more data than necessary to investigate a crime
- [ ] Risk of retention of data for a longer period of time than necessary to investigate a crime
- [x] Risk of sensitive data being revealed to public authorities (e. g. in calls to medical services or help hotlines)
- [ ] Risk of misinterpretation of data
- [x] Risk of access to data by unauthorised third parties (data breaches)
- [ ] Risk of misuse of the data for other purposes than initially intended
- [x] Risks of interference with the privacy of users
- [ ] Information security related risks
- [ ] Increased costs due to storage and technical and organisational requirements
- [ ] Customer's trust in services
- [x] Other

If other, please specify: "All of them"

It is frustrating that the Commission only allows to pick 5 of these concerns when they are all valid in case of data retention.

We suggest to focus on the ones we picked above as they cover the spectrum of risks posed by data retention, namely:

- Disproportionate interferences with the rights to privacy and data protection, in particular when sensitive data or data from which intimate information can be inferred are retained and accessed.
- Disproportionate interferences with other rights impacted by the chilling effect of permanent surveillance
- Cybersecurity risks – The Chinese State-backed attacks by Salt Typhoon targeting the US telecommunications networks show how hackers use metadata and led the US authorities to urge Americans to use encrypted services.

One trick to bypass the restricted choice is to select "other" and specify: "all of them". Note that you only have 255 characters maximum to specify if you select "other".

FUNDAMENTAL RIGHTS

12. Which investigative method requiring prior authorisation by a judge or independent administrative authority would you consider more intrusive? Please list the options in order of priority

Initial order is as follows

⠿Accessing metadata of a communication service stored by the service provider for all users

⠿Live interception of communications of targeted users

⠿Extraction of data from seized devices such as mobile phones or laptops of suspects

⠿Covert and/or undercover surveillance measures of suspects

⠿House search of suspects

We recommend to leave "Accessing metadata of a communication service stored by the service provider for all users" at the top of the list to make the point that access to metadata generally reveals a lot of information about a person, and can be used to create a detailed profile of that person's private life.

This information can be even more sensitive than the contents of communications (live interception) in terms of privacy intrusion, for example a detailed mapping of a person's social contacts or presence at sensitive locations (political demonstrations, places of worship, etc).

Moreover, metadata is highly structured (e.g. social contacts and location), which facilitates cataloguing and monitoring of large groups of persons through access to retained data, something that would not be possible to the same extent with live interception of communications content.

This question is manipulative as it forces you to create a hierarchy between intrusive measures, when it should actually be evaluated in the specific circumstances of a criminal case, as the necessity and the proportionality of the interferences with fundamental rights need to be assessed on a case-by-case basis. Furthermore the list of measures is biased as it obviously seeks to portray access to metadata as less intrusive in comparison to others, "more intrusive" ones. As a result, the "relatively" less intrusive nature (according to the Commission) of access to metadata would justify to (sometimes) bypass judicial authorisation.

This argumentation is core to the Commission's push for mass data retention of traffic and location data. It is claimed that the non-availability of data (resulting from the absence of data retention obligations) pushes law enforcement authorities to resort to more privacy-invasive tools such as spyware and wiretapping. This is highly misleading as it is comparing a mass surveillance scheme, which interferes with everyone's fundamental rights without suspicion on a permanent basis, and the interference with an individual's rights suspected in the course of a specific criminal investigation (which can be necessary and proportionate under the appropriate legal framework).

Furthermore it has been proved multiple times (see here and here) that even a limited amount of metadata can reveal very intimate details of a person's life, which was ultimately confirmed by the Court of Justice.

13. In your opinion, are there measures which would be less intrusive and still allow for the effective investigation and prosecution of crimes?

The answer is yes.

14. If yes, what could those measures be – and why would they be preferable?

255 character(s) maximum

We suggest an answer along these lines (219 characters):

"With sufficient resources and swift procedures, quick freeze orders, complying with all the applicable EU and national procedural safeguards, could effectively access data strictly necessary for a specific investigation."

In the 2020 EC study, law enforcement give a negative view of quick freeze which provides less flexibility than retention and is more cumbersome because two authorisations are required, one for preservation and one for the subsequent access. However, none of these objections from these survey respondents come even close to demonstrating the necessity of mandatory data retention over the less intrusive preservation orders. The lack of necessity is further reinforced by the fact that the success rate for law enforcement data access requests depends very little on whether there is a mandatory data retention regime or not.

Conceivably, many Member States have failed to adequately develop their quick-freeze provisions because they prefer mandatory data retention, and thus far they have been able to ignore the rulings from the CJEU that EU law precludes general and indiscriminate data retention (of all traffic data and location data).

SCOPE

15. In your opinion, to which of the following service providers should EU measures on retention of metadata be applicable?

We recommend to select "no" for all types of services providers as mandatory data retention measure will likely contravene the CJEU requirements, lead to mass surveillance and has not been proven to be necessary.

16. In your view, to investigate which types of crimes should the obligation to retain data be required?

We recommend to select "None". See explanation above.

17. In your view, should data retention requirements differ (for example the duration of the retention) depending on the type of data and the purpose of the investigation?

We recommend to select "No opinion". See explanation above.

18. Do you have any other feedback in relation to this initiative that you would like to share? (Please use the option below to upload any position papers or other relevant documents)

You are offered the possibility to submit further resources or papers if relevant.