

# Mapping CJEU limits on data retention frameworks

## A basic introduction

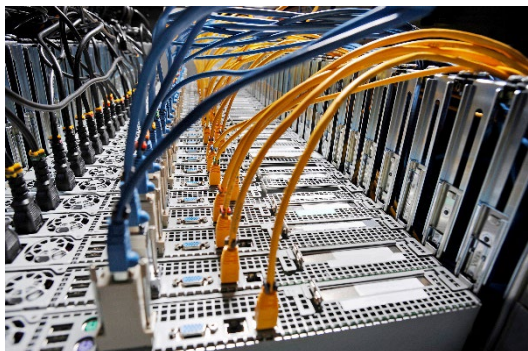
### SUMMARY

Since the 2014 invalidation of the Data Retention Directive, the EU legal landscape has become fragmented, causing uncertainty for providers and challenges for law enforcement. With a Commission proposal likely and growing Member State support for a more permissive EU regime, a solid understanding of relevant CJEU case law may help inform Parliament's assessment.

Over the past decade, CJEU case law has set detailed requirements for data retention. Laws must respect proportionality and necessity, with a clear hierarchy of objectives: general and indiscriminate retention of traffic and location data is only permissible for safeguarding national security, while targeted retention of such data may be justified by public security or other important public interest goals. Any such framework must also include robust safeguards. Similarly, access to retained data must be limited to the purpose for which it was collected or a more important objective. The ECtHR ruled that such retention and access require safeguards similar to those for secret surveillance.

Stakeholders are divided on a new EU data retention regime. Law enforcement agencies favour EU-level harmonisation but warn against restrictive retention rules that would limit their operational effectiveness. Providers of electronic communications services support a CJEU-compliant EU framework and seek cost compensation. Civil society organisations oppose new EU rules and urge the Commission to focus on enforcing existing case law through infringement procedures.

*This is one of four publications that explore different aspects of the roadmap for effective and lawful access to data for law enforcement. These include a summary of the [roadmap](#), and briefings on [lawful interception](#), [data retention](#) and [digital forensics](#).*



### IN THIS BRIEFING

- Introduction
- Background
- Parliament's position
- CJEU requirements and safeguards
- Member States' positions
- Stakeholder views
- Outlook
- Annex: Summary table of case law



## Introduction

The first EU [Data Retention Directive](#) was adopted in 2006 to create a common scheme for the retention of personal data generated or processed by electronic communications services providers, in order to make it available when investigating and prosecuting serious crimes. It took several years before Member States transposed the directive into national law. In 2014, the Court of Justice of the European Union (CJEU) struck down the directive in its landmark [Digital Rights Ireland](#) judgment, on the grounds that the 'mass, indiscriminate' retention of personal data permitted by the directive constituted a disproportionate interference with the fundamental rights to data protection and privacy.

The debate on the establishment of a new EU-wide data retention regime has intensified in recent years, with the Council repeatedly calling<sup>1</sup> for the adoption of such a framework. While the Juncker Commission did not want to put forward a [new proposal](#) for EU legislation on the matter, the von der Leyen I Commission indicated that it was more open to [considering](#) the possible development of a data retention policy. It was reported that the Commission [consulted](#) Member States in June 2021 on the future [direction](#) of data retention policy.

In June 2023, the Commission launched the [High-Level Group](#) (HLG) on access to data for effective law enforcement, which was co-chaired by the rotating Council presidency. The HLG [considered](#) a harmonised approach to data retention at the EU level essential for ensuring the effectiveness of investigations, particularly those involving cross-border elements, and for safeguarding the admissibility of evidence in judicial proceedings. In May 2025, the Commission [launched](#) a call for evidence for an impact assessment on data retention and is following it up with a public consultation. In its [Roadmap for lawful and effective access to data for law enforcement](#), the Commission summarises the situation:

*Since the EU Data Retention Directive was invalidated in 2014, the EU legislative landscape on obliging service providers to store data has become fragmented and uneven. Member States' data retention frameworks diverge on the types of electronic communications that service providers have to retain, the categories of data they cover, and the required retention periods. Moreover, some Member States do not have any data retention laws. Law enforcement and judicial authorities face legal and operational obstacles in conducting their work. Electronic communication providers, especially smaller providers, also face additional costs and obstacles when providing their services across the EU because they are required to comply with different legal requirements in different Member States.*

*The High-Level Group therefore recommended setting up a harmonised EU framework for data retention to ensure that the digital evidence required to investigate and prosecute crimes is available. A harmonised EU regime would aim at limiting fragmentation between Member States as regards the rules on retention and the safeguards pertaining to fundamental rights, in particular, privacy and data protection and the rights of defence, including the right to a fair trial. Such a legal framework would thereby also ensure legal certainty for the competent authorities, on one hand, and service providers on the other.*

The HLG [report](#) further details the issues at stake and its [recommendation](#) sets out the key features proposed for an EU data retention framework. Accordingly, an EU data retention framework should:

- I. *be technology neutral and future-proof,*
- II. *cover[...] 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. *[be] in full compliance with data protection and privacy rules.*

Since these steps are characteristic of the preparation of a legislative initiative, Parliament may soon be required to take a position on a Commission proposal concerning data retention. Given that certain Member States and law enforcement authorities would prefer to disregard certain standards set by the CJEU, it is crucial to develop a clear understanding of the relevant CJEU case law, which may serve as a benchmark to assess any future Commission proposal (for a full review of cases, see the summary table in the Annex).





## Background

Technically speaking, **mass surveillance regimes** operate in at least two different ways. They either set out the standards for tapping into and storing large volumes of data drawn from the bearers carrying internet communications ('**bulk interception**'). Or they require electronic communications service providers ('CSPs') to carry out general or targeted **retention** and storage of users' [communications data](#) and allow national authorities to have access to those data, either in a limited or unlimited fashion, often based on targeted requests. **Generalised retention** implies that all or the majority of communications data is retained without any differentiation, limitation, or exception being made. **Targeted retention** means that the retention of data is limited, for instance, through temporal, personal, or geographical limitation criteria. The retention of such data by providers, the subsequent access by authorities, and other intermediate processing operations constitute separate interferences with the fundamental rights to data protection and privacy as well as freedom of expression. The interference is of a particularly serious nature where precise conclusions can be drawn concerning individuals' private lives.

In the EU, lawmakers, courts, and commentators often refer to the particular types of communications data, notably to subscriber, traffic and location data. Traffic data and location data are formally defined in Article 2 of the [ePrivacy Directive](#). A European Commission [study](#) surveying Member States' data retention frameworks and practices defines them as follows:

- **Subscriber data** includes information that identifies the sender of a communication, such as their name, address, username, or phone number. In certain Member States, this also extends to personal details like ID number, nationality, and date of birth.
- **Traffic data** refers to information necessary to determine the type, timing, and duration of a communication, as well as details that enable the identification of the recipient or intended recipient.
- **Location data** comprises information that reveals the physical location of the communication device – for example, the position of a cell tower or Wi-Fi hotspot.

Figure 1 – Type of non-content data retained by national providers for law enforcement purposes

 <b>Subscriber data</b>		 <b>Traffic data</b>	
Name	100%	Date & time of communication	100%
Physical address	100%	Duration of communication	92%
Telephone number	100%	Start of communication	92%
Billing and payment information (e.g. client number)	100%	End of communication	92%
Email address	92%	Data volume of communication	92%
Username	69%	Type of network technology	92%
Other (e.g. ID number, date of birth)	23%	Type of communication	77%
 <b>Identification data</b>		Identifiers of the account/device to which the communication was sent.	62%
IP address	92%	Identifiers of the account/device to which the communication was forwarded or transferred.	54%
Device identification numbers (e.g. IMEI)	92%	Missed calls	54%
SIM number	85%	Connection to the service	46%
Port number for dynamic IP address	62%	Disconnection from the service	38%
 <b>Location data</b>		Identifiers of the account/device to which the communication was attempted to be forwarded or transferred.	23%
Location of the equipment or line at the start of the communication	77%		
Location of the equipment or line at the end of the communication	38%		

Source: Milieu, [Study on the retention of electronic communications non-content data for law enforcement purposes](#), European Commission, September 2020.

## Parliament's position

Parliament has continuously [advocated](#) for a high level of data protection in legislative and non-legislative procedures. In view of (at the time) 28 different legal frameworks on data retention, Parliament adopted a [resolution](#) in December 2018 urging the Commission to evaluate a new legislative proposal on data retention that upholds the principles of purpose limitation, proportionality and necessity. Two years later, Parliament focused its attention on compliance. In its November 2020 [resolution](#), it called on the Commission to initiate infringement proceedings against Member States that had failed to repeal national transposition acts of the annulled Data Retention Directive. In its [resolution](#) of March 2021, Parliament urged the Commission to apply the conclusions of the CJEU case law, including *La Quadrature du Net I* and *Privacy International*, to all reviews of adequacy decisions as well as ongoing and future negotiations. In the context of the [Pegasus spyware scandal](#), Parliament set up a committee of inquiry and, in its [recommendation](#) of June 2023, derived key standards for spyware surveillance operations from CJEU case law relating to data retention.

## CJEU requirements and safeguards

### The invalidation of the Data Retention Directive

In a decade-long line of cases, the CJEU has shaped a set of EU standards for data retention frameworks. This process began with the 2014 landmark judgment ***Digital Rights Ireland*** (Joined

cases [C-293/12](#) and [C-594/12](#)). The Court annulled the [Data Retention Directive](#), on the grounds that it imposed a general and indiscriminate obligation on electronic communications services providers to retain all traffic and location data for at least six months and up to two years for the purpose of the prevention, investigation, detection and prosecution of serious crime. The CJEU considered that the interference caused by the Directive with the fundamental rights to data protection and private life was particularly serious and could not be justified for reasons of combating serious crime.

The Court insisted that data retention may be ordered only when it is strictly necessary for a legitimate objective. EU legislation would have to establish clear, precise rules on the scope and application of the retention measure, and impose minimum safeguards to ensure that retained data was protected against abuse, unlawful access, and misuse. The CJEU concluded that the Directive failed to pass the necessity test, because it (1) required the indiscriminate retention of data (by providers of public electronic communications services) without adequate temporal, personal, or geographical limitations (i.e. targeting), (2) lacked limits on data access and subsequent use by competent authorities, and (3) did not sufficiently differentiate the retention period of six to 24 months.

Specifically, the Directive lacked safeguards to prevent the **retention** of non-relevant and privileged data (e.g. data of uninvolved parties or data protected by professional secrecy), and to limit retention to what is strictly necessary for fighting serious crime (time period, geographical zone and target groups). As regards **access** and use of data by competent authorities, the Directive failed to define a common threshold for serious crime, impose strict purpose limitation and data minimisation requirements, and require prior authorisation of access. Lastly, necessity fails, because the Directive failed to differentiate the minimum **retention** period (by data type, data relevance and persons concerned) and failed to define objective criteria for determining the proportionate retention period within the statutory range.

Additionally, the Directive failed to ensure effective protection of retained data against abuse, unlawful access, and misuse, due to the absence of data security, data deletion and data localisation requirements.

## Reviewing national data retention laws against the EU data *acquis*

### *Tele2 Sverige and Watson*

In its 2016 **Tele2 Sverige and Watson** judgment (joined cases [C-203/15](#) and [C-698/15](#)), the CJEU ruled that the ePrivacy Directive precludes national laws requiring general and indiscriminate retention of all traffic and location data for crime fighting purposes, as well as laws that grant authorities access to such data without proper safeguards and conditions. The CJEU established that the ePrivacy Directive applies to national data retention schemes, and further develops necessary conditions and safeguards for data retention and access to this data.

Reflecting the *Digital Rights Ireland* judgment, the court clarified that Member States can mandate as a preventive measure the **targeted retention** of traffic and location data for the purpose of fighting serious crime, if targeting is appropriately restricted with regard to the categories of data, the means of communication affected, the persons concerned and the retention period. Additionally, during targeted retention of traffic and location data, providers have to ensure a particularly high level of data security, retain data within the EU, and irreversibly destroy data at the end of the data retention period. Member States have to ensure that an independent authority reviews compliance with EU data protection standards.

In addition, **access** to the retained traffic and location data by the competent authority must be subject to adequate conditions and safeguards. Given the seriousness of the interference, the Court

ruled that such access must be limited to objectives related to combating serious crime as opposed to ordinary crime. Furthermore, access may not exceed the limits of what is strictly necessary, a court or independent administrative body must review the competent authority's decision to access the data, and authorities must notify the data subject about the access where this no longer risks jeopardising the operation.

## Ministerio Fiscal

The 2018 judgment *Ministerio Fiscal* (Case [C-207/16](#)) addressed whether and to what extent authorities can access certain subscriber data to identify owners of SIM cards activated with stolen phones. The Court acknowledged that it had previously ruled that access to traffic and location data must be limited to combating serious crime, but clarified that this applies only when there is serious interference with fundamental rights. Less serious interference can be justified for preventing and prosecuting criminal offences in general. Thus, the Court found that access to basic data like names and addresses may be justified for this purpose.

## La Quadrature du Net I

In its 2020 *La Quadrature du Net I* judgment (Joined [Cases C-511/18, C-512/18 and C-520/18](#)), the CJEU synthesised and developed its findings of previous rulings. It clarified that the ePrivacy Directive even applies to national laws imposing data retention on electronic communications for **national security purposes**. Additionally, the Court distinguished six to seven data retention-related processing operations and clarified limitations and safeguards for each.

The Court established that national legislation may empower authorities to order electronic communications services providers to **retain data generally and indiscriminately**, provided that the measure is conditional on countering a genuine and present or foreseeable threat to national security. The measure must be limited in time to what is strictly necessary and subject to effective review either by a court or by an independent administrative body. Additionally, data retention must be circumscribed by safeguards against the risk of abuse and other – so far undetermined – limitations. Consequently, while the general and indiscriminate retention of data is possible, it may not be systematic.

The Court also reaffirmed that **targeted retention of traffic and location data** – including retention limited to IP addresses providing insights into individuals' private lives – is permitted only for tackling serious crime or addressing serious threats to public security. While such data must usually be erased or made anonymous, there is the possibility for **expedited preservation of such data** under certain circumstances. Authorities may **access traffic and location data** retained by providers only where it serves the same, or a more significant, public interest objective as that which initially justified the data retention. In contrast, **retaining basic identity data** may be justified for preventing and investigating ordinary criminal offences.

Essentially, the judgment establishes a hierarchy of objectives, allowing more intrusive retention or access measures only when authorities pursue more significant goals. '[T]he importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference'.<sup>2</sup>

Besides that, the judgment also clarifies that **automated analysis of traffic and location data** to screen data for retention is only permitted where it is necessary to prevent genuine and present or foreseeable threats to national security. The **real-time collection of traffic and location data** linked to persons reasonably suspected of being involved in terrorist activities are only possible under strict conditions.

## La Quadrature du Net II

In its *La Quadrature du Net II* judgment of 2024 (Case [C-470/21](#)), the CJEU considered whether the EU data *acquis* precludes national laws which allow a copyright enforcement authority to access civil identity data retained by providers of electronic communications services and linked to an IP address used in suspected criminal activity, for the purpose of pursuing copyright violations.

Access necessarily presupposes that the requested data is retained, so the Court first clarified under which conditions national law may impose the **retention** of IP addresses and civil identity data on providers of electronic communications services. Differentiating or overturning its line of reasoning in *La Quadrature du Net I*, the Court clarified that the retention of IP addresses does not always constitute a serious interference. Such retention may be justified for the purposes of combating ordinary crime and safeguarding public security, provided that the interference is considered general in nature. This is the case where a Member State is able to rule out the combination of those IP addresses with other data that would potentially allow the entity to draw precise conclusions about the individual's private life by imposing a range of organisational and technical measures. Member States must 'guarantee a genuinely watertight separation of the different categories of data retained' and its reliability 'must be subject to regular review'.

Subsequently, the Court established that authorities may be authorised to **access** civil identity data retained by providers and linked to an IP address used in suspected criminal activity. This is contingent on the data having been retained specifically for that purpose, on providers being required to store it in a way that prevents the revelation of private life details (see above), and on the condition that such access does not amount to a serious interference with fundamental rights. Whether access presents a serious interference depends on the context, such as whether the combination of requested data and other data available to the requesting authority is liable to reveal precise conclusions about an individual's private life, and whether appropriate confidentiality safeguards are in place. The Court indicated that, where the interference is serious, such as when authorities can draw precise conclusions about an individual's private life by combining the requested data with other data available to them, retention and access could only be justified based on combating serious crime and, *a fortiori*, the safeguarding of national security. In contrast, safeguards reducing the seriousness of interference include limiting data access by personnel, prescribing confidentiality obligations on officials, prohibiting officials from tracking IP address holders and imposing purpose limitations.

Generally, the Court held that prior review is not required where the interference is not serious. However, in graduated (tiered) administrative procedures concerning the same individual, the copyright enforcement authority would repeatedly request access and gain increasing amounts of data and insights relating to the individual. Where an advanced procedure is reached that is liable to allow the public authority to draw precise conclusions about an individual's private life, the national legislation must foresee a prior review of an authority's decision to access the data.

### Box: European Court of Human Rights (ECtHR) requirements and safeguards

The ECtHR has dealt with several data retention cases and frequently refers to CJEU case law, notably when determining the level of interference and corresponding proportionate objectives. In [Breyer v. Germany](#), the ECtHR considers that the legal mandates to retain and access limited subscriber information was lawful, given that it qualified as **limited interference** (analogous to *Ministerio Fiscal*), provided for sufficient safeguards, and was limited to what is necessary. In subsequent case law, the ECtHR dealt with frameworks governing the retention of and access to metadata that were liable to reveal an intimate picture of an individual and thereby qualified as **intrusive**. In [Ekimdzhiev and Others v. Bulgaria](#), the Court examined safeguards for **access** and **storage** of collected data and ruled that general retention of communications data and its access by authorities must be subject to safeguards equivalent to those for secret surveillance.

In [Škoberne v. Slovenia](#) and [Pietrzak and Bychawska-Siniarska and Others v. Poland](#) the ECtHR applied this reasoning to the upstream data **retention**. In *Škoberne v. Slovenia, para. 137*, the ECtHR summarised that its case law on surveillance in **criminal investigations** has developed minimum safeguards that must be set out in law to prevent abuse: *'the nature of offences that may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed .... In Roman Zakharov ... – which concerned, in addition, other public-interest aims, such as the protection of **national security** – the Court framed the applicable safeguards along similar lines, with further emphasis placed on the notification mechanisms and the remedies provided by national law .... Within the context of bulk interception relating to international communications, in Big Brother Watch and Others ... and Centrum för rättvisa ..., the Court further adjusted the aforementioned criteria ...'*

## Member States' positions

### Reception of CJEU case law

Since the *Tele2* judgment, Member States have adopted divergent approaches<sup>3</sup> to data retention, resulting in a fragmented legal landscape across the European Union. While the majority of Member States maintain some form of data retention regime, the scope, structure, and legal basis of these regimes vary significantly. Many Member States have [indicated](#) that efforts are still under way to assess and revise existing data retention and access rules.

According to a [report](#) by Eurojust and ECJN, half of the Member States have amended existing laws or introduced new measures aimed at aligning with the requirements articulated by the Court. Conversely, a number of Member States have yet to enact new legislation following the annulment of their previous data retention frameworks.

Many Member States continue to apply data retention laws that do not meet the CJEU's targeting requirements, though several have introduced (partially) targeted legislation in recent years. Most of these Member States use specific categories of data as a targeting criterion. One Member State bases retention obligations on geographic areas with elevated crime rates, while others focus on the particular means of communication, such as telephone data. Some permit general data retention only for limited categories – such as subscriber information or IP addresses – or for specific purposes, notably national security. A few have introduced expedited retention measures, requiring service providers to preserve data that would not otherwise be subject to retention.

Time limits for data retention also vary considerably between Member States, reflecting differing national interpretations of necessity and proportionality.

Alongside changes to retention regimes, several Member States have revised access provisions, particularly regarding the authorities empowered to authorise access and the thresholds defining the seriousness of the offence for which access may be requested. The minimum imprisonment sentence used to define 'serious crime' varies between Member States.

## The political positions of Member States

The following overview highlights the political stances and legal interpretations adopted by selected Member States.

In preparation for the HLG on access to data, in 2023 **Estonia** [highlighted](#) the practical difficulties of implementing the CJEU's prescribed alternatives to general data retention. It argued that targeting criteria are impractical and fail to meet the needs of law enforcement. Estonia supports a broader balancing of fundamental rights, including the right to security, life and health, besides the right to privacy and data protection. It calls for an EU-wide mapping of national legislation and supports the development of a harmonised regulatory framework.

**France** strongly [contested](#) the CJEU's jurisprudence on data retention, viewing it as incompatible with national security imperatives. French institutions, from the Council of State to the Court of Cassation, have resisted fully implementing the Court's decisions over many years. Despite having made changes, France continues to uphold broad data retention measures justified by persistent terrorist threats (as consecutively evidenced by the general prosecutor since 1994). In the run-up to the HLG, France [insisted](#) that the group should not aim to translate the CJEU case law into policy, but rather propose realistic and operational solutions that reflect law enforcement realities.

In a similar vein, academics have [chronicled](#) **Ireland's** apparent reluctance to comply with the CJEU rulings. Despite changes made to bring national data retention regimes into compliance with the *Commissioner of An Garda Síochána* ruling, the changes have been criticised for failing to address the fundamental flaws identified in the 2017 '[Murray Review](#)' of the previous legislation.

In 2023, **Slovakia** [advocated](#) reviving a common EU legislative solution that would introduce at least minimum retention capabilities for law enforcement to obtain telecommunication data necessary for criminal investigations, while also imposing firm safeguards to regulate access and prevent misuse. Slovakia argued that the CJEU case law has resulted in a disproportionate emphasis on the right to privacy, at the expense of fundamental rights of crime victims. It contends that reframing the terminology used in these discussions could help shift political perceptions within the European Parliament, which would be essential for enabling future reforms of the relevant secondary legislation as interpreted by the CJEU.

**Germany** has taken a cautious and legally conservative [approach](#) to data retention. Since 2010, data retention has been effectively defunct, and attempts to reinstate general retention schemes have failed. Germany supports a European approach that [complies](#) with the CJEU's case law and the EU Charter of Fundamental Rights. The previous coalition government (SPD, Greens, FDP) endorsed ad hoc retention subject to judicial approval, which some interpret as a rejection of general and indiscriminate data retention. The new [coalition](#) between the SPD and the CDU/CSU now plans to introduce a three-month retention of IP addresses and port numbers, in order to enable their attribution to subscribers.

In 2021, the **Netherlands** [underlined](#) that it remains vocally supportive of a new EU-wide data retention regime, despite domestic inaction on the issue. Previously, the Dutch government had [expressed concern](#) over the 'regrettable constraints imposed by CJEU case law'. Deliberations within the High-Level Group are closely monitored.

The **Danish** Presidency of the Council places high [strategic](#) importance on access to data for law enforcement, especially in tackling technology-enabled crime. The Presidency announced that it will

'focus on access to data for effective law enforcement and the obligations of providers to process data for law enforcement purposes'. It will also follow up on the implementation of the EU internal security strategy. In 2021, Denmark [stated](#) that it supports a common EU approach to data retention and that 'the EU legislators should define the way forward on a subject as important as data retention rather than leaving the regulation to the ECJ'. It cautioned against further limiting the scope for retention – particularly regarding national security. If future legislation were to reflect the CJEU position in a limiting way, Denmark would favour no EU action.

As shown in the table below, Member States also gave an indication of their preference for the design of an EU data retention scheme in the [Commission consultation](#) of 2021.

Figure 2 – Preferred legislative design

Member state	Type of approach		Type of retention				
	Leg.	Non-leg.	National security	Targeted	Quick freeze	IP	Civil identity
Denmark	-	?	X	?	?	?	?
Finland	?	?	?	?	X	?	?
Germany	✓	?	✓	X	X	✓	?
Hungary	✓	X	X	X	+	X	X
Luxembourg	✓	X	?	?	?	?	?
Netherlands	✓	+	X	?	+	?	✓
Sweden	✓	?	X	X	?	✓	✓

Source: Statewatch, [Data retention strikes back? Options for mass telecoms surveillance under discussion again](#), 1 December 2021.

## Stakeholder views

In their 2025 joint report [Common Challenges in Cybercrime](#), **Europol and Eurojust** emphasised that legal uncertainty resulting from the invalidation of the Data Retention Directive still hinders the availability of data for investigations. The joint report also warns that traffic data are routinely deleted before requests arrive, delaying or derailing investigations and undermining cross-border cooperation due to the absence of a common EU data retention framework.

Telecom and online-service providers, represented by [Connect Europe and the GSMA](#), submitted a joint response to the Commission's call for evidence on 18 June 2025 stressing the operational difficulties caused by the fragmented data retention landscape across EU Member States and uncertainty about compliance of national laws with CJEU case law. They warn that general long-term obligations on data retention would be costly and that a new regulation should provide for a cost compensation mechanism. New rules should avoid prescribing operational details, allowing flexibility in the technical implementation.

Microsoft (Ares(2025)4860730) welcomes the Commission's efforts to address the fragmented state of data retention laws, and supports the creation of a harmonised framework, provided that it upholds fundamental rights and accounts for technical limitations. However, Microsoft points out that any new data retention scheme should be limited to what is necessary for the investigation and prosecution of serious crimes and should only cover basic subscriber information and traffic data that is already stored by the provider. Any data retention mechanism should be duly balanced with the providers' fundamental freedom to conduct business. This may require exceptions for SMEs or B2B providers, for whom retention obligations may be too burdensome.

On the other hand, digital rights advocacy organisations, led by European Digital Rights (EDRi), submitted a [joint civil society response](#) to the Commission's call for evidence opposing any proposal for new EU legislation that would require electronic communications providers to store large amounts of users' traffic and location data beyond what is essential for providing the service or for billing-related reasons. They call on the Commission to prioritise the launching of infringement proceedings against Member States whose data retention laws are not aligned with CJEU case law.

The European Data Protection Board (EDPB), in its [statement of 4 November 2024](#) on the HLG's recommendations, welcomed the idea of a harmonised EU framework on data retention, provided it is fully compliant with the CJEU case. However, it expressed concerns over the suggestion that data retention obligations should cover all present and future data handlers, which could extend general retention duties to a wide range of service providers and result in de facto mass surveillance. The EDPB stressed that the CJEU's reasoning in the *La Quadrature du Net II* ruling, justifying the general retention of IP addresses, cannot be used to justify wider retention of other types of revealing data such as traffic and location data.

## Outlook

The future of data retention in the EU remains highly contested. Since the invalidation of the Data Retention Directive in 2014, the legislative landscape has become fragmented, creating legal uncertainty for providers and operational difficulties for law enforcement authorities.

A number of Member States have expressed support for reviving an EU-level data retention instrument with several favouring a model based on a permissive interpretation of CJEU case law, or even a departure from it.

Efforts by lawmakers to carve out exemptions for certain data retention practices<sup>4</sup> from the scope of EU law carry significant risks. It is likely that civil society organisations would perceive this as an attempt to roll back the established EU fundamental rights protection. Additionally, even if certain practices are framed as purely national under secondary law, they remain subject to scrutiny under the European Convention on Human Rights. In the same vein, the CJEU has shown a clear willingness to defend the reach of fundamental rights in any area where Member States are [implementing](#) EU law.<sup>5</sup> The design, cost, and effectiveness of such an approach require careful consideration.

Even if the current scope of EU law remains unchanged, significant legal [uncertainty](#) surrounds the interpretation of CJEU case law. This ambiguity does not give legislators carte blanche. Any new data retention framework must carefully balance fundamental rights. To withstand judicial scrutiny, future legislation must be proportionate. Relevant factors may include evidence that data retention is effective in achieving the objective of combating serious crime, the availability of alternative investigative tools, and the burden on service providers. Given recent concerns about the misuse of spyware and the centralisation of US databases, enhanced safeguards against misuse and 'function creep' could be considered. Exceeding the margin of appreciation or neglecting adequate safeguards risks invalidation of the framework by the CJEU, especially in light of likely strategic litigation and the lowered admissibility thresholds before the CJEU and ECtHR in data retention cases.

## ENDNOTES

- <sup>1</sup> T. Wahl, [The Awakening of EU Data Retention Rules](#), Eucriim, 2019; T. Wahl, Council: [The Way Forward in Data Retention](#), Eucriim, 2019; European Commission, [Call for evidence for an impact assessment](#), Ares(2025)4081079, May 2025.
- <sup>2</sup> *Commissioner of An Garda Síochána*, paras. 53 and 56; See also *LQDN I*, para. 131 and *Privacy International*, para. 75.
- <sup>3</sup> E. Kosta and I. Kamara, [Data Retention in Europe and Beyond](#), Oxford University Press, pp. 117–294; General Secretariat of the Council (leaked), [Data retention – Situation in Member States](#), WK 3103/2019 INIT, March 2019; Milieu, [Study on the retention of electronic communications non-content data for law enforcement purposes](#), European Commission, 2020; Eurojust and EJCNC, [The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU](#), report, November 2024; A. Birrer, 'The state is watching you—A cross-national comparison of data retention in Europe', *Telecommunications Policy*, Vol. 74(4), 2023, no. 102542; Marianna Mattera, [Data Retention](#), Cullen International, July 2025; European Union Agency for Fundamental Rights, [Data retention across the EU](#), July 2017.
- <sup>4</sup> For instance, they might attempt to remove data retention for the purpose of national security from the scope of the ePrivacy Directive and other applicable secondary laws such as data protection laws.
- <sup>5</sup> [Mayer](#), [Schlikker](#), [Bäcker/Moini](#), and [Boehm/Cole](#) indicate that mass surveillance programmes and data retention schemes may interfere with the EU fundamental freedoms and thus trigger the application of EU fundamental rights. This avenue is especially relevant for data retention scenarios that are exempt from the scope of EU secondary law. Applicants [raised](#) the matter with the German Constitutional Court; however, as it was not decisive for the merits of the case the Court did not rule on it (paras. 65–66 and 328). [Ewer/Thienel](#) oppose the notion that such mass surveillance regimes would interfere with the fundamental freedoms.

## DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2025.

Photo credits: © sonjanovak / Adobe Stock.

[eprs@ep.europa.eu](mailto:eprs@ep.europa.eu) (contact)

<https://eprs.in.ep.europa.eu> (intranet)

[www.europarl.europa.eu/thinktank](http://www.europarl.europa.eu/thinktank) (internet)

<http://epthinktank.eu> (blog)

Annex: Summary table of case law<sup>6</sup>

Processing mandate	Legitimate objectives	Limitations and exceptions to the scope of retention (targeting)	Retention period or period in respect of which access is sought	Prior review	Notification duties	Other conditions
A legislative measure empowering authorities to instruct e-coms services providers to carry out general retention of traffic and location data (LQDN I) or of the majority of traffic and location data for several weeks <sup>7</sup> (SpaceNet)	Genuine, serious and present or foreseeable threat to national security (LQDN I, para. 137, <i>An Garda Síochána</i> , paras. 62-63; ECtHR, <i>Pietrzak and Bychawska-Siniarska</i> , paras. 256-262, esp. para. 259).	A threat to national security may establish the relevance <sup>8</sup> of collecting all data for the objective of safeguarding national security (LQDN I, para. 137). <sup>9</sup>	Limited in time to what is strictly necessary with the possibility of renewal where justified, e.g. threats persist (LQDN I, para. 138).	Authorities' decision to impose retention must be subject to effective prior review, either by a court or by an independent administrative body (LQDN I, paras. 139).		Data retention must be subject to limitations and may not be systematic (LQDN I, para. 138; ECtHR, <i>Škoberne v. Slovenia</i> , paras. 140 and 142).  Safeguards against data abuse (LQDN I, para. 138).
A legislative measure imposing targeted retention obligation of traffic and location data <sup>10</sup> (LQDN I)	Combating serious crime, safeguarding public security, and safeguarding national security (LQDN I, para. 146; <i>Prokuratuur</i> , para. 33). Member States cannot distort <sup>11</sup> the concept 'serious crime' ( <i>Procura di Bolzano</i> , paras. 44-63).	Legislation must ensure, via objective criteria, that only data strictly necessary and relevant to the objective is retained, e.g. using geographical, personal, temporal, or other distinctive limits (LQDN I, paras. 143-144 and 148-150; <i>DRI</i> , paras. 57-59; <i>Tele2</i> , paras. 110-111; <i>An Garda Síochána</i> , para. 83; <i>SpaceNet</i> , paras. 112-113).	Limited in time to what is strictly necessary with the possibility of renewal where justified (LQDN I, paras. 147 and 151). Data must be irreversibly destroyed at the end ( <i>Tele2</i> , para. 122 and <i>DRI</i> , para. 67) or anonymised (LQDN I, para. 160 and <i>An Garda Síochána</i> , para. 85).			Safeguards against the risk of misuse ( <i>Tele2</i> , para. 109; <i>DRI</i> , para. 66)  Data must be retained within the European Union ( <i>Tele2</i> , para. 122; <i>DRI</i> , para. 68)

<p>A legislative measure empowering authorities to instruct e-coms services providers to carry out expedited retention of traffic and location data (<i>LQDN I</i>)</p>	<p>Combatting serious crime and, a fortiori, the safeguarding of national security. (<i>LQDN I</i>, para. 164).</p>	<p>To limit interference to what's strictly necessary, retention must be restricted by objective criteria like geographical, personal, or temporal limits. Retention may be ordered at an early stage of an investigation of a serious threat or crime. (<i>LQDN I</i>, paras. 164-167; <i>An Garda Síochána</i>, para. 90-91 and <i>SpaceNet</i>, para. 120)</p>	<p>Limited to a specified period of time (<i>LQDN I</i>, paras. 163 and 168; <i>An Garda Síochána</i>, para. 86)</p>	<p>Authorities' decision to impose retention must be subject to effective judicial review (<i>LQDN I</i>, para. 163; <i>An Garda Síochána</i>, para. 86).</p>	<p>Legislation must provide effective safeguards against the risks of abuse and against any unlawful access to or use of those data (<i>LQDN I</i>, para. 168).</p>
<p>A legislative measure granting authorities access to traffic and location data retained by e-coms services providers (<i>Tele2</i>; <i>Prokuratuur</i>) (see the rows above)<sup>12</sup></p> <p>A legislative measure empowering authorities to oblige e-coms services providers to forward retained traffic and location data to intelligence agencies (<i>PI</i>)</p>	<p>Only justifiable by the objective for which it may be retained (<i>DRI</i>, para. 61; <i>Tele2</i>, para. 115; <i>LQDN I</i>, paras. 158 and 166; <i>LQDN II</i>, para. 97; <i>Prokuratuur</i>, para. 35; <i>Ministerio Fiscal</i>, para. 54; ECtHR, <i>Škoberne v. Slovenia</i>, para. 144; ECtHR, <i>Pietrzak and Bychawska-Siniarska</i>, para. 263) or for a more important public interest objective, e.g. safeguarding national security (<i>LQDN I</i>, para. 166 and <i>LQDN II</i>, para. 97).<sup>13</sup></p>	<p>Access must follow objective criteria and be strictly necessary and proportionate. For crime fighting, it should mainly target individuals suspected or implicated in serious offences, allowing access to non-suspects' data only in exceptional<sup>14</sup> cases. (<i>Tele2</i>, para. 119; <i>PI</i>, paras. 77-80; <i>Prokuratuur</i>, paras. 38 and 49-50; <i>An Garda Síochána</i>, paras. 103-105; <i>Spetsializirana prokuratura</i>, paras. 65 and 67; <i>LQDN I</i>, paras. 165-167; and <i>DRI</i>, para. 61-62)</p>	<p>The competent authority must ensure that the period in respect of which access is sought is limited to what is strictly necessary for the purposes of the investigation (<i>Prokuratuur</i>, para. 38; <i>Procura di Bolzano</i>, para. 36; <i>LQDN II</i>, para. 95).</p> <p>Clear time-limits for destroying data accessed in the course of criminal proceedings are necessary (ECtHR, <i>Ekimdzhev</i>, para. 408).</p>	<p>Access decision must be subject to prior review by a court or an independent<sup>15</sup> administrative body, except in cases of duly justified urgency. (<i>Tele2</i>, para. 120; <i>DRI</i>, para. 62; <i>LQDN II</i>, paras. 123-128 and 131; <i>Prokuratuur</i>, paras. 51 and 58; <i>An Garda Síochána</i>, para. 106). The authorisation procedure must ensure access to data is proportionate (ECtHR, <i>Ekimdzhev</i>, paras. 400-406).</p>	<p>Persons affected must be notified as soon as that notification is no longer liable to jeopardise the investigations (<i>Tele2</i>, para. 121; <i>Spetsializirana prokuratura</i>, paras. 70-71 and 76; ECtHR, <i>Ekimdzhev</i>, paras. 416-417).</p> <p>Effective oversight must be ensured (ECtHR, <i>Ekimdzhev</i>, paras. 410-415 and 395 and 291-292).</p> <p>If access is authorised without hearing the person concerned, notification and remedies are required. (<i>Spetsializirana prokuratura</i>, paras. 75-76)</p> <p>Clear rules must govern the handling and destruction of accessed data (ECtHR, <i>Ekimdzhev</i>, para. 409)</p> <p>Additional safeguards apply to journalist data or likely collateral intrusion (ECtHR, <i>BBW</i>, paras. 524-525 and see 442-445)</p>

<p>A legislative measure imposing general retention of IP addresses - only of the sender/source, not the receiver (e.g. <i>LQDN I</i>; <i>SpaceNet</i>; <i>LQDN II</i>)</p>	<p>IP address retention is a serious interference if combining it with other contextually available data could reveal private life details and is then only justifiable for combating serious threats or crime or safeguarding national security (<i>LQDN I</i>, paras. 152–156; <i>SpaceNet</i>, para. 103; <i>LQDN II</i>, paras. 80–81). Where legislation rules out sensitive private life insights by providing for a watertight separation of data, retention may also serve general crime prevention. (<i>LQDN II</i>, paras. 82–92, 103).</p>	<p>Even in the absence of a specific connection between all users of e-coms systems and the objectives pursued, Article 15 ePD permits the general retention of IP addresses for legitimate objectives. (<i>LQDN II</i>, para. 92).</p>	<p>The legislative measure must ensure that the retention period is limited to what is strictly necessary in light of the objective pursued (<i>LQDN II</i>, para. 93 with reference to <i>LQDN I</i>, para. 156 and 168)</p>			<p>Effective safeguards against the risks of abuse and against any unlawful access to or use of those data must be ensured. (<i>LQDN II</i>, para. 93 with reference to <i>LQDN I</i>, para. 168)</p>
<p>A legislative measure imposing general retention of civil identity / subscriber data (<i>LQDN I</i>)</p>	<p>Preventing, investigating, detecting and prosecuting criminal offences in general (<i>LQDN I</i>, para. 158; <i>SpaceNet</i>, para. 99).</p>	<p>Article 15 ePD allows general retention of civil identity data, even without a specific link to the objective pursued. (<i>LQDN I</i>, para. 155). Data must help to clearly identify the relevant subscriber (ECtHR, <i>Breyer</i>, para. 96).</p>	<p>No time limit is required for retaining certain civil identity data (<i>LQDN I</i>, para. 159; however, see ECtHR, <i>Breyer</i>, para. 96).</p>			<p>Effective safeguards against the risks of abuse and against any unlawful access to or use of those data must be ensured. (<i>LQDN I</i>, para. 168)</p>

<p>A legislative measure authorising a public authority to access civil identity data retained and linked to an IP address used in suspected copyright infringements (<i>LQDN II</i>)</p> <p>or</p> <p>to telephone numbers and identity data of SIM card holders that was retained (<i>Ministerio Fiscal</i>)</p>	<p>Access may be granted for combating certain ordinary offences for which the data was retained (<i>LQDN II</i>, paras. 96 and 102; <i>Ministerio Fiscal</i>, paras. 57 and 62) or for a more important public interest objective (<i>LQDN I</i>, para. 166; <i>LQDN II</i>, paras. 97-98). Access to telephone numbers and SIM card identity data may be justified for combating criminal offences generally (<i>Ministerio Fiscal</i>, paras. 48-63). For civil identity data linked to a suspicious IP address, the required objective depends on the interference level: where access contextually poses a risk of revealing private life insights, a significant public interest is needed; otherwise,<sup>16</sup> ordinary objectives may suffice (<i>LQDN II</i>, paras. 97, 101-112 and 146).<sup>17</sup></p>	<p>Access may not go beyond what is necessary (<i>LQDN II</i>, paras. 113, 118 and 127; ECtHR, <i>Breyer</i>, para. 100).</p>	<p>The requirement of necessity is met where access to data is limited to what is necessary and this necessity requirement is safeguarded by a general obligation to erase, without undue delay, any data that is not needed (ECtHR, <i>Breyer</i>, para. 100; for serious interferences, cf. <i>LQDN II</i>, para. 95).</p>	<p>Prior review is not required when access to personal data by public authorities does not constitute a serious interference (<i>LQDN II</i>, paras. 129-134 and 144). However, in tiered (graduated) procedures, such as those escalating from warnings to prosecution, authorities may gain access to additional data, increasing the risk of revealing sensitive aspects of an individual's private life. In such cases, national law must ensure prior review<sup>18</sup> by a court or independent body at advanced stages. (<i>LQDN II</i>, paras. 135-141 and 143). The review cannot be automated (<i>LQDN II</i>, paras. 147-151).</p>	<p>Under the LED a notification is required, doing so is liable to prejudice the investigations or another derogation applies (<i>mutatis mutandis Spetsializirana prokuratura</i>, para. 71; <i>Bara and Others</i>, paras. 39-41; and <i>Bezirkshauptmannschaft Landeck</i>, paras. 111-123). The ECtHR held that a notification is not required where a legal order provides for supervision by independent DPAs and appeals procedures (ECtHR, <i>Breyer</i>, paras. 102-107).</p>	<p>Legislation must include effective safeguards against the risks of abusive or unlawful access to or use of those data (<i>LQDN II</i>, para. 152).</p> <p>In advanced stages of tiered procedures, where combined data may reveal private life details, safeguards must prevent automatic linking of civil identity with IP data (<i>LQDN II</i>, para. 142)</p> <p>Automated processing may be used but must undergo regular review by an independent body (<i>LQDN II</i>, paras. 153-156).</p> <p>Under the LED, individuals in graduated response procedures (e.g. Hadopi) must have access to rights such as access, rectification, and erasure, a complaint procedure with an independent supervisory authority, and judicial remedy (<i>LQDN II</i>, paras. 152-163).</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>A legislative measure requiring providers to implement measures allowing the automated analysis of traffic and location data (as general and indiscriminate processing, <i>LQDN I</i>, paras. 169, 172)</p>	<p>Genuine and present or foreseeable threat to national security (<i>LQDN I</i>, para. 177)</p>		<p>The duration of the [subsequent] retention must be limited to what is strictly necessary. (<i>LQDN I</i>, para. 177)</p>	<p>The decision authorising automated analysis must be subject to effective review, either by a court or by an independent administrative body whose decision is binding. (<i>LQDN I</i>, para. 179)</p>	<p>The authority must publish general information about the automated analysis, but individual notification is required if a person is identified for deeper analysis based on matching data. (<i>LQDN I</i>, para. 191)</p>	<p>Pre-established models and on which that type of data processing are based should be specific, reliable, and non-discriminatory. (<i>LQDN I</i>, para. 180)</p> <p>Automated analysis must not rely on pre-established models or differentiation criteria based solely on sensitive data. (<i>LQDN I</i>, para. 181)</p> <p>Any positive result from automated processing must be individually re-examined by non-automated means before any adverse measure is taken. (<i>LQDN I</i>, para. 182)</p>
<p>A legislative measure requiring providers to implement measures allowing the real-time collection of traffic and location data relating to persons suspected of being involved in terrorist activities (<i>LQDN I</i>, para. 169)</p>	<p>Real-time collection of traffic and location data is allowed only for persons reasonably suspected of terrorism. For others, only non-real-time access is permitted, and only where evidence shows it could significantly aid counter-terrorism. (<i>LQDN I</i>, para. 188).</p>	<p>The legislative measure must clearly define when data collection is authorised and ensure it applies only to individuals demonstrably linked to preventing terrorism (as outlined in the adjacent cell to the left). (<i>LQDN I</i>, paras. 188 and 189)</p>		<p>The decision to authorise real-time collection must be subject to a prior review carried out either by a court or by an independent administrative body. In cases of duly justified urgency, the review must take place within a short time. (<i>LQDN I</i>, para. 189)</p>	<p>Persons concerned must be notified as soon as doing so no longer risks undermining their operations. (<i>LQDN I</i>, para. 190)</p>	<p>A decision authorising the real-time collection of traffic and location data must be based on objective and non-discriminatory criteria provided for in national legislation. (<i>LQDN I</i>, para. 189)</p>

- <sup>6</sup> This table provides an overview of data retention case law but does not aspire to offer an exhaustive account of all applicable requirements and safeguards. The absence of judicial rulings on certain safeguards does not imply that they are expendable. The ECtHR ruled that general retention of revealing communications data and its access by authorities must be subject to safeguards equivalent to those for secret surveillance (for details, see the box on page 8). Further information on safeguards can be drawn from [reports](#) by the [FRA](#) and the [Venice Commission](#). Unless otherwise specified (e.g. ECtHR), references to case law concern CJEU rulings.
- <sup>7</sup> When the data intended for retention is liable to reveal insights on the private life of the persons concerned, see *Spacenet*, paras. 88–89.
- <sup>8</sup> On the requirement for an objective connection, see *Tele2*, para 110.
- <sup>9</sup> Limited access with due safeguards cannot legitimise unlawful generalised retention (*Commissioner of An Garda Síochána*, para. 47; ECtHR, [Škoberne v. Slovenia](#), paras. 144; ECtHR, [Pietrzak and Bychawska-Siniarska and Others v. Poland](#), para. 262).
- <sup>10</sup> Insofar as the data intended for retention is liable to reveal insights on the private life of the persons concerned, mutatis mutandis *Prokuratuur*, paras. 39–40, *Spacenet*, paras. 88–89, and *LQDN II*, para. 81.
- <sup>11</sup> E.g. by including within it offences which are manifestly not serious offences.
- <sup>12</sup> Insofar as the data intended for retention is liable to reveal insights on the private life of the persons concerned, see *Prokuratuur*, paras. 39–40.
- <sup>13</sup> Combating serious crime cannot permit access to data that was retained generally and indiscriminately for safeguarding national security (*Commissioner of An Garda Síochána*, paras. 96–100; *SpaceNet*, paras. 126–130; ECtHR, [Škoberne v. Slovenia](#), paras. 144; ECtHR, [Pietrzak and Bychawska-Siniarska and Others v. Poland](#), para. 263). The fact that the requested access to traffic or location data relates only to a short period does not lessen the seriousness of the interference when that set of data is liable to allow precise conclusions to be drawn concerning the private life of the persons concerned, nor does it remove the need for a justification based on an important public interest objective (*Prokuratuur*, paras. 39–40 and *Procura della Repubblica presso il Tribunale di Bolzano*, para. 40).
- <sup>14</sup> When terrorist activities pose a significant threat to national security, defence, or public safety—it may be justifiable to grant access to the data of individuals not directly suspected of criminal activity.
- <sup>15</sup> Neither the public prosecutor's office, nor a police officer, assisted by a unit established within the police service which enjoys a degree of autonomy, meet these requirements (*Prokuratuur*, paras. 54–57; *Commissioner of An Garda Síochána*, paras. 111–114). By contrast, the ECtHR held that a legal framework allowing authorities to access existing records of operators on calls made and received as well as the cell towers used by a phone line, which is subject to prior authorisation from the prosecutor and ensures judicial review, are compliant with the European Convention on Human Rights (ECtHR, [Ben Faiza c. France](#), paras. 73 and 79–80).
- <sup>16</sup> To avoid an interference of a serious nature requiring justification by particularly important public interest objectives, the access and retention regime must ensure that e-coms services providers organisationally and technically isolate the IP addresses retained (*LQDN II*, paras. 97 and 102–104) and that the accessing authority cannot typically draw revealing conclusions by combining the accessed data with other contextually available data (*LQDN II*, paras. 107–112). Other measures capable of reducing the degree of interference include limiting the number of officials authorised to access data; imposing binding confidentiality obligations and adopting other safeguards (*LQDN II*, paras. 113–114 and 164).
- <sup>17</sup> This sentence should not be understood as expressing a position on the [implications](#) of the *LQDN II* judgment for IP address retention.
- <sup>18</sup> Where the person concerned is suspected of having committed the minor offence of 'gross negligence', the court or independent administrative body responsible for reviewing the access request (necessary only in advanced procedural stages) must refuse access if it would enable authorities to draw precise conclusions about the individual's private life (*LQDN II*, para. 145). By contrast, such access may be authorised where the suspicion concerns counterfeiting, as Member States may classify it as a serious crime (*LQDN II*, para. 146).