Council of the European Union

Brussels, 13 December 2024
(OR. en)

16844/1/24
REV 1

COPEN 547
EUROJUST 97
JAI 1870

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	The effect of case-law of the Court of Justice of the European Union on national data retention regimes and judicial cooperation in the EU - Joint report by Eurojust and the European Judicial Cybercrime Network

Delegations will find attached the above-mentioned report. It is also available on the website of Eurojust.

The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU

November 2024

Criminal justice across borders

EUROJUST

European Union Agency for Criminal Justice Cooperation

EUROPEAN JUDICIAL CYBERCRIME NETWORK

Contents

1. Purpose

At the beginning of 2017, the College of Eurojust initiated a project designed to assess the impact on judicial cooperation in criminal matters within the European Union (EU) of the judgment of the Court of Justice of the European Union (CJEU) in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson* ([1]). The project aimed to get an overview of the legal frameworks in the Member States relating to the retention of traffic and location data, along with the access to such retained data by law enforcement and judicial authorities. It also included practitioners' views on the impact of the CJEU judgment on cross-border investigations and prosecutions. The outcome of this mapping exercise was presented in the first report on data retention regimes in Europe ([2]).

One of the findings of this report was that '… the data retention legislative framework has either been changed, is currently being reviewed and/or has been subject to developing judicial precedent in a significant number of countries …'. Given the continuous legislative developments and differences in national data retention regimes, it was concluded at the time that the developments and the potential impact of the CJEU judgment, both on a national level and in the area of judicial cooperation in criminal matters, should be further monitored. Case-law has also evolved in the meantime, as the CJEU has rendered new judgments in relation to data retention.

After several years of monitoring relevant developments ([3]), it was decided in 2023 to perform another impact assessment with a view to preparing a second report. Similarly to the first report, a questionnaire was sent to the European Judicial Cybercrime Network (EJCN) ([4]) for this purpose. The analysis of the replies to the questionnaire is presented in the current report, which gives an update on the topic of data retention, including practitioners' views on the matter. As the first report did, it aims to provide an overview of data retention regimes in the Member States and serve as an experience-based contribution to the assessment of the impact of the CJEU rulings on cross-border judicial cooperation in criminal matters.

2. Methodology

For this second report, the same methodology was used as for the first report. A detailed questionnaire was sent to the members of the EJCN in August 2023. In order to be able to compare the main findings and conclusions of the first report and to see the evolution in this area over the years (2016–2024), it was decided to ask the same questions that were used for the first report in 2017 (see Annex 1).

All 27 Member State representatives of the EJCN provided their replies to the questionnaire between the end of 2023 and the beginning of 2024.

([1]) Judgment of the Court of Justice of 21 December 2016, *Tele2 Sverige and Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.

([2]) Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15, 6 November 2017, LIMITE.

([3]) Monitoring of legislative and case-law developments on data retention via the yearly *Cybercrime Judicial Monitor*.

([4]) The EJCN was established by Council Conclusion of 9 June 2016 (10025/16) with the objective of facilitating the exchange of expertise and best practice, enhancing cooperation between the competent judicial authorities when dealing with cybercrime, cyber-enabled crime and investigations in cyberspace, and fostering dialogue to ensure the rule of law in cyberspace. Eurojust provides support to the EJCN in organising meetings, maintaining the restricted access website of the network, facilitating the day-to-day activities of the Board and assisting in the implementation of the work programme.

The questionnaire covers the legal framework governing data retention and strives to approach the issue from the perspective of judicial cooperation, particularly among Member States. Emphasis was accordingly placed on questions relating to the legislative structure of national data retention regimes, whether the legal framework provided for general/mass indiscriminate data retention, the scope of the safeguards relative to access to data and, finally, the possible impact of the judgment on the collection and admissibility of evidence domestically and on judicial cooperation in general.

For the sake of this questionnaire, the term 'data retention' applies to non-content data (subscriber information, traffic, location and other transactional data) retained by electronic communications service providers. Unless indicated differently, the focus of this report is on data retention for law enforcement purposes.

The report provides information on the current legal landscape concerning data retention in the EU, and aims to assess the impact of the CJEU case-law on the collection of evidence and judicial cooperation in criminal matters. It does not provide a detailed overview of each of the national legal systems, but rather aims at highlighting the main changes, differences and challenges that have occurred across Member States over the past several years, along with significant and interesting aspects worth mentioning in relation to the focus of this report. From the impact assessment that has now been conducted over a longer period of time, and based on the findings of both data retention reports, some conclusions will be drawn at the end.

3. Background information

Already in 2015, following the CJEU ruling in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* ([5]), practitioners raised concerns about the potential issues that could arise from the absence of a harmonised EU legal framework on data retention ([6]). Indeed, after the invalidation of Directive 2006/24/EC and the subsequent CJEU judgment in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson*, data retention laws in many Member States were annulled or amended. This not only resulted in a disperse legal landscape in the EU, but it also left law enforcement and judicial authorities faced with different types of challenges in relation to the gathering, accessing and use of data in criminal investigations and prosecutions, in both national and cross-border contexts. Subsequent CJEU case-law continues to influence legal developments at the national level.

In support of its operational casework, Eurojust needed to have better insight into the challenges encountered by practitioners in this area and remain up to date with the legal developments in the Member States. Hence, Eurojust has been following the legal and case-law developments related to data retention closely since 2015.

([5]) Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.

([6]) Eurojust, Meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union and Workshop on Data Retention in the Fight Against Serious Crime: The Way Forward, Conclusions, The Hague, 10 and 11 December 2015.

Over the past several years, the CJEU has rendered several judgments in relation to data retention, thereby further clarifying the requirements for EU legislation when it comes to the retention of data by service providers and the access to such data by law enforcement authorities for the purpose of criminal investigations.

In its ruling in *Tele2 Sverige and Watson*, the CJEU found that EU law **precludes the general and indiscriminate retention of traffic data and location data**. However, Member States are free to regulate data retention, in a targeted manner. Such retention should be limited to what is strictly necessary, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the chosen duration of retention. **Access of national authorities to the retained data** is restricted to the objective of fighting serious crime and must be subject to conditions, including prior review by an independent authority.

In 2017, Eurojust assessed the impact of this ruling on EU data retention regimes and on potential challenges encountered in criminal investigations and prosecutions, including cross-border judicial cooperation. The results and conclusions of this exercise were reported in the first data retention report.

The Court reiterated and further clarified its earlier standpoint in subsequent rulings, thereby creating an increasingly detailed line of case-law in this area.

In its judgment of 2 October 2018 in Case C-207/16, *Ministerio Fiscal* ([7]), the CJEU indicated that **access** to retained traffic and location data can be justified for criminal offences in general, if it does not constitute a serious interference with a person's fundamental rights.

The CJEU repeated the prohibition of general and indiscriminate retention of traffic and location data in Case C-511/18, *La Quadrature du Net and Others* ([8]), but did state that **some legislative measures are allowed, for specific purposes and under certain conditions**:

- Instructions requiring **general and indiscriminate retention of traffic and location data** in situations where the Member State concerned is confronted with a **serious threat to national security** that is shown to be genuine and present or foreseeable. The decision imposing the instruction must be subject to effective review by a court or an independent administrative body.
- **Targeted retention** of traffic and location data, limited to the categories of persons concerned or using a geographical criterion, for a period that is limited in time.
- General and indiscriminate retention of **IP addresses assigned to the source of an internet connection** for a limited period of time.
- General and indiscriminate retention of **data relating to the civil identity of users of electronic communications systems**.
- Instructions requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the **expedited retention** ([9]) **of traffic and location data** in the possession of those service providers.

([7]) Judgment of the Court of Justice of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788.
([8]) Judgment of the Court of Justice of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791.
([9]) Expedited retention is also referred to as 'quick-freeze'.

These measures should ensure that the data retention at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

The CJEU further stipulated that automated analysis and real-time collection of traffic and location data by service providers is only allowed in specific situations and under certain conditions.

Moreover, national criminal courts also need to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where:

— those persons are not in a position to comment effectively on that information and that evidence; and

— the information and/or evidence pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.

The CJEU reiterated these elaborated principles in further rulings rendered in 2022, Case C-140/20, *Commissioner of An Garda Síochána* ([10]), and Joined Cases C-793/19 and C-794/19, *SpaceNet and Telekom Deutschland* ([11]).

In Case C-746/18, *Prokuratuur* ([12]), the Court further clarified that **access** to a set of traffic or location data, allowing precise conclusions to be drawn concerning a person's private life, **is allowed only in order to combat serious crime or prevent serious threats to public security**, regardless of the duration of the access and the quantity or nature of the data. Moreover, a **public prosecutor cannot** be granted the power to **authorise access** of a public authority to traffic and location data for the purposes of a criminal investigation, as **prior review** of such access should be done by a **court or an independent administrative body**.

4. Analysis of the replies to the questionnaire

4.1. Mandatory data retention for criminal investigation purposes: legislation

The EJCN members were asked about the domestic legislation governing data retention for law enforcement purposes in their Member States, and whether any legislative changes had taken place since 2018 ([13]). The analysis of the replies showed that the CJEU case-law has indeed further impacted the legal landscape in Europe.

([10]) Judgment of the Court of Justice of 5 April 2022, *Commissioner of An Garda Síochána*, C-140/20, ECLI:EU:C:2022:258.
([11]) Judgment of the Court of Justice of 20 September 2022, *SpaceNet and Telekom Deutschland*, C-793/19 and C-794/19, ECLI:EU:C:2022:702.
([12]) Judgment of the Court of Justice of 2 March 2021, *Prokuratuur*, C-746/18, ECLI:EU:C:2021:152.
([13]) Legislative changes before 2018 were reported in the previous report.

Twelve Member States (BE, DK, EE, IE, FR, HR, IT, LV, LT, PT, SK, SE) made key changes to their legislation between 2018 and 2022. Respondents replied that these changes were a direct result of CJEU Case C-746/18, *Prokuratuur*, and Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*. Before the legislative changes, these Member States had legal provisions in place that entitled the public prosecutor or law enforcement to authorise access to data overall and/or targeted data retention was not provided for in the law.

The changes carried out by the indicated Member States consisted of both amendments of legal provisions and the introduction of completely new legal provisions regulating the subject matter.

The remaining 15 Member States indicated that they did not make any significant changes to their country's regulations between 2018 and 2022. It is also worth mentioning here that a small group of Member States (EL, ES, CY) indicated that their current regulations are still based in essence on the invalidated Directive 2006/24/EC.

A small number of Member States indicated that they do not currently have in place mandatory data retention rules for the purpose of criminal investigations (DE, NL, RO, SI). These countries have to rely on the availability of data gathered for business purposes by service providers.

Data retention regulations are usually incorporated into electronic telecommunication laws and/or criminal procedure codes. A compilation of data retention laws can be found in Annex 2.

4.2. From general and indiscriminate data retention to targeted data retention

To determine whether data retention provisions in the Member States are of a general nature or targeted in the sense of the CJEU ruling, respondents were asked whether the provisions in their country contained restrictions concerning the categories of data (traffic and location data) to be retained, the users or subscribers and the means of communication. Therefore, general limitations such as the time period for which the data needs to be retained, or the general indication of the purpose to prevent and fight crime, are not considered to be targeting conditions as interpreted by the CJEU. These latter restrictions apply to all data retained under national schemes.

Some respondents indicated that they considered their data retention regime to be targeted by virtue of these general limitations. For the purpose of this analysis, we have therefore interpreted the answers on the basis of the content of the legislation, when possible.

Looking at the targeting criterion, the Member States can be grouped as follows.

— Half of the respondents replied that there are no targeted data retention rules in their Member State in terms of categories of data (location/traffic data), users or means of communication (internet/telephone).

— Many Member States already have rules in place aligning with the requirements of the CJEU, including targeted data retention rules. However, the manner in which the targeting criteria have been introduced differs significantly among the Member States. In some Member States, the targeting criterion is linked to the type of data as such, while in others it is based on geographical conditions. In some countries, the retention of traffic and location data is fully prohibited. In most of these Member States, general and indiscriminate data retention rules are, to a greater or lesser extent, still in place for the retention of certain types of data (identity and subscriber data, source IP addresses) or for specific purposes (e.g. threat to national security), whether or not this is a result of the CJEU case-law.

  In this context, the following data retention regimes were reported in more detail.

  - **Austria.** The Austrian Code of Criminal Procedure has introduced the targeting criterion for traffic, access and location data only. The code stipulates that such data may not be stored or transmitted, except in the cases explicitly regulated by law (quick-freeze). Traffic data must be deleted or anonymised as soon as the payment process has been completed and the charges have not been contested in writing within a period of 3 months. Content data must be deleted or made anonymous by the provider immediately after the connection has been terminated ([14]).

    The storage of targeted data in the sense of Article §134 Z 2b StPO has to be understood as the refraining from the deletion of traffic, access and location data. This measure is intended to trigger an obligation for service providers not to delete data that has already been collected and thus to secure later access to this data in the course of criminal proceedings.

  - **Belgium.** Following a ruling of the Belgian Constitutional Court on 22 April 2021 ([15]), detailed changes were introduced to the Belgian legislation in 2022, de facto creating a so-called layered system. This system determines what electronic data has to be gathered and retained by the service providers, indiscriminately or in a limited manner, in which regions, during what time period, who can access it and for what purposes.

([14]) Article §134 Z 2b of the Austrian Code of Criminal Procedure, https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326&FassungVom=2024-10-17&Artikel=&Paragraf=134&Anlage=&Uebergangsrecht=.

([15]) Judgment of the Belgian Constitutional Court of 22 April 2021, https://www.const-court.be/public/n/2021/2021-057n.pdf.

Certain types of electronic data (metadata) have to be gathered and retained by the service providers systematically for a certain period (mentioned below) for reasons of national security or to combat serious crime in certain geographically limited areas.

— Six, 9 or 12 months in all areas where the level of serious crimes surpasses a set number. The length of the retention period depends on the level of crime (the statistics used to determine which level was attained are verified by the data protection authority for the police).

— Twelve months in areas where the threat level for national security is 3 or higher (determined by the Coordination Unit for Threat Analysis on a scale of 1 to 4).

— Twelve months in areas particularly vulnerable for reasons of national security or serious crime (e.g. airports, ports, governmental agencies, etc.) ([16]).

In addition, certain types of identity data still have to be gathered and retained in a general and indiscriminate manner, for a period of 12 months ([17]).

Traffic and location data can also be subject to a request for expedited retention (quick-freeze). This measure can be ordered for a period of 2 months and can be extended to a maximum of 6 months ([18]).

- **Denmark.** The Danish Administration of Justice Act was amended in 2022. The act now provides for the following ([19]):

  — Targeted retention of traffic and location data for the purpose of combating serious crime (imprisonment of at least 3 years) or preventing serious attacks on public security. The targeting criterion concerns **specific locations or individuals**. The retention period is 1 year.

  — General and indiscriminate retention of traffic and location data if the state is confronted with a serious threat that is shown to be genuine and present or foreseeable. The retention period is 1 year.

  — General and indiscriminate retention of information related to a user's access to the internet (IP address). The retention period is 1 year.

- **France.** In France, general and indiscriminate retention of data is prohibited, except in the following cases:

  — Retention of traffic and location data if there is an actual, predictable and serious threat to national security. The retention period is 1 year.

  — Retention of identity data and subscriber data for the purpose of conducting criminal procedures and to prevent threats to national security. The retention periods are respectively 5 years and 1 year.

([16]) Article 126/3 of the Law of 13 June 2005 on electronic communications, https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=05-06-20&numac=2005011238.
([17]) Article 126 of the Law of 13 June 2005 on electronic communications, https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=05-06-20&numac=2005011238.
([18]) Article 39 § 5 of the Belgian Code of Criminal Procedure, https://www.ejustice.just.fgov.be/img_l/pdf/1808/11/17/1808111701_F.pdf.
([19]) Sections 786 b–f of the Administration of Justice Act.

— Retention of source connection data (IP address), for the purpose of fighting serious crimes and preventing threats to national security. The retention period is 1 year.

— For the purpose of fighting serious crime, a judicial authority may also order a quick-freeze of traffic and location data held by service providers.

- **Ireland.** The Communications (Retention of Data) (Amendment) Act 2022 amended the existing Communications (Retention of Data) Act 2011. The law now provides as follows:

  — The general and indiscriminate retention of communications traffic and location data may only be permitted on national security grounds, where approved by a designated judge following an application by the Minister for Justice in circumstances where the minister is satisfied that there exists a serious and genuine, present or foreseeable threat to national security ([20]).

  — Preservation and production orders may be obtained by An Garda Síochána (the Irish police) to facilitate the preservation of and access to specified communications data held by service providers for both national security and the investigation of serious crime, where permitted by an authorising judge.

Draft legislation on the protection, preservation and access to data on information systems is also currently in the Irish legislative process (see Section 4.4 below).

- **Portugal.** In February 2024, a new law introduced amendments to the provisions regulating the retention of and access to electronic communications data. In essence, only identity data, basic subscriber information and IP addresses can be retained for the purpose of investigating and prosecuting serious crimes (imprisonment of at least 5 years). The new law further developed the concept of 'serious crime' ([21]).

  It is prohibited to retain traffic and location data, except in the case of a prior judicial authorisation issued for the purpose of combating serious crime (quick-freeze) ([22]).

- **Sweden.** On 1 October 2019, new data retention rules entered into force that limited the retention obligation, while at the same time differentiating the retention periods.

  The rules differentiate between categories of data and means of communication.

  — For telephony and messaging, only communication via a mobile network access point should be retained. No data will be retained on telephony or messaging that takes place in the fixed-line (landline) telephone network or through fixed internet access. The retention period is 6 months.

([20]) Section 3A of the Communications (Retention of Data) Act 2011, https://www.irishstatutebook.ie/eli/2011/act/3/section/3/enacted/en/html#sec3.

([21]) Law 18/2024 defines serious crime as crimes of terrorism, violent crime, highly organised crime, kidnapping, hostage-taking, crimes against cultural identity and personal integrity, crimes against state security, counterfeiting of currency or currency-like securities, counterfeiting of cards or other payment devices, use of counterfeit cards or other payment devices, acquisition of counterfeit cards or other payment devices, acts preparatory to counterfeiting and crimes covered by a convention on the safety of air or maritime navigation.

([22]) Article 6 of the Law No 18 of 2024.

— Traffic data will be retained, but the obligation to retain will be limited to data on who contacted whom (number and subscriber, and for telephony also subscription and equipment numbers) and at what time. The retention period is 6 months.

— Location data at the beginning and end of a call will be retained, but no other location data. The retention period is 2 months.

— For internet access, the retention obligation includes data that makes it possible to identify the subscriber or registered user: IP addresses and other technical data necessary to identify the subscriber or registered user, time data for logging in and out of the service providing internet access, subscriber information and data identifying the equipment where the communication is finally separated to the subscriber. The retention period is 10 months ([23]).

4.3. Access to data by law enforcement and judicial authorities: safeguards

4.3.1. Prior review by a court or an independent body

The vast majority of the respondents outlined that a (prior) judicial review is required to obtain access to data stored by service providers. This prior review takes the form of an order or authorisation by a judicial authority.

There are slight differences in the way Member States have regulated this. In many Member States, such prior authorisation / judicial review falls within the competence of a **court or (investigating) judge** (BG, CZ, DK, EE, IE, EL, ES, HR, IT, CY, LT, PT, RO, SI ([24]), SK, FI). It is worth noting here that, following Case C-746/18, *Prokuratuur*, in which the CJEU stated that a public prosecutor cannot be granted the power to authorise the access to data, several Member States have amended their provisions to align them with the Court's standpoint, and thus have now given this competence to a(n) (investigating) judge (EE, IE, IT).

In several Member States, the prior review can still fall within the competence of either a **prosecutor or a judge/court**, depending on the type of data to which access is requested (BE, LU, NL) or the stage of the investigations or proceedings (FR ([25]), LV, PL ([26]), SE). The absence of prior review is overcome by proper safeguards provided for by the law (removal of evidence). In one Member State, judges, courts or prosecutors can also order or request access to data (HU). In one Member State, access to data can be ordered by a prosecutor (AT).

([23]) Chapter 9, Sections 19 and 22 of the Electronic Communications Act (2022;482), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20224 82-om-elektronisk-kommunikation_sfs-2022-482/.

([24]) Since amendments to the Slovenian Criminal Procedure Act entered into force in August 2024, it is now also possible to obtain a court order for access to subscriber data, if it allows an individual to be identified by a unique identifier that is not in the public domain or in respect of which there is a legitimate expectation of privacy.

([25]) A prosecutor can order access to data in the context of preliminary investigations or investigations in flagrante delicto. The absence of prior judicial review can only lead to annulment if the person concerned can claim a grievance. This is not the case when access is justified in light of the seriousness of the offence and the needs of the investigation.

([26]) In preparatory proceedings, the public prosecutor issues an order requesting access to data; in court proceedings, it is the court (the judge concerned) issuing an order.

One Member State indicated that prior authorisation by a court or an independent administrative authority is not needed for the police or security service to be granted access to data (MT). Given the lack of data retention regulations in Germany, the provisions for access to such data are de facto not applicable.

Several respondents replied that, if data is requested and obtained on the basis of a request by the police or a prosecutor for police inquiries or in a pre-trial stage, a court order is still required to be able to use the information as evidence in court.

4.3.2. Other conditions and substantive and procedural safeguards regarding access to data

Many respondents indicated that the granting of access to data is linked to the nature of the crime. Several Member States require a minimum threshold of penalties, or require the crime to be serious or specifically listed.

The definition of the concept of 'serious offence' – in relation to the application of the provisions of the Privacy and Electronic Communications Directive – was considered by the CJEU in its judgment in Case C-178/22, *Procura della Repubblica presso il Tribunale di Bolzano* ([27]):

'Consequently, in view of the division of competences between the European Union and the Member States under the FEU Treaty and the considerable differences between the legal systems of the Member States in the area of criminal law, it must be found that it is for the Member States to define 'serious offences' for the purposes of applying Article 15(1) of Directive 2002/58.'

Several respondents replied that the concept of serious crime or offence is not defined by their domestic law. As a result, for a fact to be considered serious crime, the minimum imprisonment term required varies among Member States, ranging from 1 to 6 years.

Other respondents mentioned that the data needs to be relevant to the proceedings and/or there needs to be an initial suspicion of a crime having been committed.

The order or request to access the data also needs to take due account of the principles of necessity and proportionality.

4.3.3. Access to data in emergency situations

Several respondents indicated that their domestic legislation provides for a mechanism for the waiver of the prior judicial review in the case of a validly established urgency, be it in the form of an explicit provision or as an exception to the requirement of prior review by a judge or court (CZ, DK, IE, EL, HR, IT, CY, LT, LU, NL, RO, FI, SE).

([27]) Judgment of the Court of Justice of 30 April 2024, *Procura della Repubblica presso il Tribunale di Bolzano*, C-178/22, ECLI:EU:C:2024:371.

In this regard, what is considered an emergency differs among Member States. In some Member States, particular circumstances could lead to an emergency situation in which access to data is required, such as missing persons or anti-terrorist investigative measures (CZ), kidnapping (CY) or serious risks to the life, liberty or physical integrity of a person (LU). Next to this, some domestic provisions envisage emergency access in case of risk of loss of evidence (DK, NL, RO), serious compromise of ongoing criminal proceedings (IT, LU) or risk to national security (EL). In one Member State, the law refers in more general terms to 'an urgent need to act' (IT).

In these emergency cases, law enforcement authorities can usually access data without the prior authorisation of a judge or court, or a prosecutor can authorise the access. The time frame within which a court needs to review the legality of the measure varies among Member States: as soon as possible (SE), within 24 hours (FI), 48 hours (HR, IT) or 3 days (LT). In Greece, pending a criminal investigation, a public prosecutor or an investigative judge may authorise access to data. The legality of the authorisation subsequently needs to be reviewed by a board of judges within 3 days. In some Member States, authorisation by a judge or prosecutor can be given orally, but needs to be confirmed in writing within 24 hours (LU) or 3 days (NL).

The remaining respondents did not indicate having specific provisions in place in their domestic law relating to access to data in emergency situations.

Although there is no specific domestic provision for accessing data in emergency situations in Spain, there is a provision that allows the judicial police or a prosecutor to request identification data directly from service providers. This provision can also be applied in emergency situations. Following a similar line of reasoning, one could argue that the provisions on data access in some Member States that give competence to the prosecutor to authorise access could be applied in emergency situations as well.

4.4. Developments related to national legal frameworks on data retention

In 9 Member States, work is ongoing to amend or introduce new legislation in relation to data retention, ranging from ongoing discussions to the quite advanced drafting of new legislation (DE, EL, FR, EE, IE, LU, NL, LV, SE).

- In **Germany**, the government has decided to propose a quick-freeze solution, but discussions are still ongoing with a view to adopting new data retention laws.
- In **Greece**, the CJEU case-law triggered a debate on new legislation in this area.
- In **France**, the Ministry of Justice is considering a legislative change relating to the conditions of access to traffic and location data in the context of criminal investigations to comply with the case-law of the CJEU and ensure legal certainty. A working group was set up for this purpose, which completed its work in June 2024. The recommendations contained in the working group's report are still under discussion and arbitration.
- In **Estonia**, the Appeal Court has rendered evidence inadmissible as the law does not comply with the rulings of the CJEU. As a result, work has been initiated to prepare a new law.

— In **Ireland**, draft legislation on the Protection, Preservation and Access to Data on Information Systems is currently in the Irish legislative process. Subject to legislative scrutiny, this legislation may further clarify procedures for access to data held by internet service providers ([28]).

— In **Luxembourg**, the legal framework on data retention will be changed. Bill of law No 8148 on retention of personal data is currently being debated in the Chamber of Deputies, with the aim of implementing the procedural requirements stemming from the case-law of the CJEU ([29]). General and indiscriminate retention of data will be repealed, with the exception of IP addresses and data related to the civil identity of users. Retention of traffic and location data will be limited to certain geographical zones, based on the number and frequency of serious crimes.

— In the **Netherlands**, a new Code of Criminal Procedure will enter into force in the upcoming years, which will update certain provisions. Access to traffic data will require authorisation by a judge instead of a prosecutor, which is already being applied in practice.

— In **Latvia**, amendments to the Electronic Communications Law, particularly Sections 99, 100 and 101, are underway, with a view to bringing them in line with the CJEU case-law and the Constitution of the Republic of Latvia.

— In **Sweden**, an analysis of the current regulations on data retention and access for law enforcement purposes was conducted. In May 2023, the outcome of the analysis gave reason to amend the rules in light of new case-law from the CJEU. Proposals on targeted data retention for the purpose of combating serious crime were submitted. The retention is targeted in the sense that it is limited to a specific geographical area or to a specific group of people, or distinguished by another criterion, such as a technical one. The work is ongoing.

Although there are no further ongoing legislative initiatives to amend the respective laws, it was indicated that, in two Member States, private entities and NGOs have launched appeals for annulment of the law before the constitutional courts (BE, CZ). It is worth noting that the appeal for annulment in Belgium concerned the new data retention regulations that were introduced in 2022. The Belgian Constitutional Court pronounced its ruling on 26 September 2024. It ruled on several aspects of the data retention law and decided to refer preliminary questions to the CJEU ([30]).

4.5. Collection and admissibility of evidence

Respondents were asked to identify any direct impact of the CJEU case-law on data collection and the admissibility of data as evidence in court. These questions thus pertained to the domestic impact of the CJEU rulings.

([28]) General Scheme of the Criminal Justice (Protection, Preservation of and Access to Data on Information Systems) Bill 2024.
([29]) Bill of law No 8148, 8 February 2023, https://www.chd.lu/en/dossier/8148.
([30]) This ruling was rendered at the time of finalisation of this report, which prevented the provision of an exhaustive overview of the main conclusions of the Court.

Several respondents indicated that the CJEU rulings have had an impact on the **availability of data** in their Member State for the purpose of criminal investigations. Different aspects of the rulings (limitations to types of data retained, authorising judicial authority for access, crime categories required for access and data retention periods) were mentioned as the reason for the unavailability of data. The following examples were provided:

- In Ireland, since the new regulations restrict retention of traffic and location data to a specific significant need (national security) that cannot always be determined or defined, there is less data available.
- In Italy, an impact on the availability of data is noticeable since access to data is now restricted to certain crimes.
- There have been instances where Slovak courts did not accept the motion of a prosecutor to issue an order to obtain data. Moreover, data retained for business purposes by service providers is often only kept for a short time period, so that it is not available.
- In France, the number of requests for access sent to service providers dropped significantly after the Court of Cassation rulings (see below).
- In Cyprus, following a ruling of the Supreme Court, the police can have access to IP addresses, but not to any telecommunication data from telephones.
- Short data retention periods in Sweden have affected the availability of location data. Such data is needed to match with a suspect's smartphone in cases where decrypted messages from EncroChat and Sky ECC ([31]) are used as evidence.

In Germany, the absence of a data retention regime has also affected the availability of data for criminal investigations ([32]).

In most Member States, it is possible and permitted to use **data that has been stored legitimately by service providers for their own purposes** for criminal investigation purposes, as long as it is obtained following the procedural requirements prescribed by law. Four respondents replied that this would not be possible in their Member State (BG, CY, PL, SE). Although the type of data available might be limited or partially different from the data required by law enforcement in an investigation, the use of such data could provide a practical solution to the unavailability of data in some cases. On the contrary, as observed by one respondent (RO), the data processed (for business or other purposes) may vary from one provider to another. As a result, in some cases, this data is not useful for criminal investigations. Moreover, the absence of a data retention regime can cause a lot of uncertainty among service providers as to what data could still be gathered and provided to the authorities, as was observed in Belgium, in the period between the annulment of the previous law and the entry into force of the new law.

Two respondents mentioned that investigations have already been discontinued because of the unavailability of data (IE, SK).

([31]) Encrypted communication platforms used by criminals.

([32]) This is irrespective of the CJEU rulings, as there has been no mandatory data retention in force in Germany since 2008.

As was already noticeable soon after the CJEU ruling in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson*, the impact of the case-law of the CJEU has been mostly visible and continued to be visible in the context of assessing the **admissibility of evidence** in court (court of first instance, appellate court, supreme court or appeal of convictions). Several Member States have reported on court rulings in which the admissibility of the data gathered in a case was assessed.

In Belgium, courts have practically unanimously adopted the same reasoning when confronted with a claim that the evidence was collected illegally under the previous law ([33]). National courts have found that there is no breach of the law that prescribes the limited instances in which irregularly obtained evidence needs to be declared null and void. Moreover, when assessing the admissibility of illegally obtained evidence in light of Articles 6 European Convention on Human Rights and 14 International Covenant on Civil and Political Rights, courts have found that there has not been a violation of the right to a fair trial. In the courts' views, the defendant had been given the opportunity to comment effectively on the information and evidence gathered. Moreover, the data gathered did not relate to an area of which the judges have no knowledge, and this data did not have a decisive impact on the assessment of the facts. Based on these considerations, courts have ruled that the telecommunications data requested from service providers should not be excluded from the evidence. The same applies to the evidence based on this telecommunications data. It is worth mentioning here that, in the context of the Sky ECC spin-off cases that are currently being prosecuted, the defence continually tries to challenge the admissibility of the telecommunications data. The Court of Cassation has already upheld the first judgments of the court of appeal, but many more cases will undoubtedly follow. In addition, the defence has already announced their plans to bring these cases before the European Court of Human Rights.

In France, the Court of Cassation has ruled on the admissibility of data retained in contravention of the terms of the CJEU ([34]). According to the CJEU, any national court ruling on the admissibility related to access to traffic and location data will have to verify that the facts involved constitute serious crime and that the quick-freeze of and access to the traffic and location data were necessary and proportionate to the prosecution of the offences concerned. Insofar as no prior review by an independent court or administrative body is envisaged (orders by a prosecutor in the context of preliminary investigations or flagrante delicto), a court only needs to decide on the exclusion of the evidence if the person affected can demonstrate an unjustified interference of their privacy. This is not the case when, in light of the seriousness of the offence and the needs of the investigation, access to connection data appears to be justified.

In Spain, several judgments have been delivered by the Supreme Court ([35]) mentioning the doctrine established by the CJEU and concluding that Spanish legislation provides for enough and adequate safeguards to ensure that access to data is only possible under the required conditions, so that the right to privacy and the right to data protection are preserved. It seems, however, that the question of whether this data has been retained under a general retention regime has not been considered in depth.

([33]) Constitutional Court ruling of 22 April 2021 and Court of Cassation rulings of 11 January 2022 (P.21.1245.N), 25 January 2022 (P.21.1353.N), 29 March 2022 (P.22.0078.N) and 29 March 2022 (P.21.1422.N).
([34]) Four rulings of the French Court of Cassation of 12 July 2022.
([35]) Rulings of the Spanish Supreme Court of 23 March 2020 (Case No 727/2020) and 19 October 2022 (Case No 824/22).

In Estonia, the Appeal Court ruled in May 2024 that traffic and location data are not admissible evidence in court proceedings, as Estonian law is not in compliance with the rulings of the CJEU (because data retention is not targeted)([36]). Currently, it is not clear what will be the impact of this decision on the ongoing proceedings and judicial cooperation in cross-border investigations.

In Ireland, two persons were convicted on the basis of traffic and location data coming from burner phones. The prosecution had asserted that the convicts could not assert privacy rights over phones they had not admitted ownership over – the Court of Appeal ruled that the public interest in the investigation, part of which involves the rights of the victims, comprehensively outweighs any limited privacy rights attached to the data accessed in the investigation. This ruling was, however, appealed to the Irish Supreme Court, which overturned the decision. It disagreed with the Court of Appeal and decided that the data or evidence had been obtained in breach of the Charter of Fundamental Rights of the European Union. They disagreed with the prosecution arguments that one could not assert privacy over material seized on a burner phone. In Ireland, a breach of domestic or EU law (always taking into account the principles of equivalence and effectiveness) does not mean the evidence concerned is mandatorily excluded. The Court can assess the admissibility of the evidence in the circumstances of each case. The Court applies criteria set down in case-law. In the circumstances of this case the Court ruled that the evidence could be admitted, and the conviction was affirmed accordingly ([37]).

In Denmark, there is a case pending before the Supreme Court. One of the arguments that needs to be assessed by the court is whether data collected in the context of a criminal investigation before the CJEU C-140/20 Case, *An Garda Síochána*, and the changes to the Danish Administration of Justice Act can be used as evidence in the criminal trial after the said CJEU ruling and amended act.

The above case-law is just a fraction of the rulings that have been rendered in the Member States over the past several years. Eurojust has been monitoring national legislative and case-law developments in relation to data retention since 2016, through its yearly *Cybercrime Judicial Monitor* ([38]). A more extensive overview of national case-law on data retention, including the judgments referenced above, can be found in these reports. From the rulings that have been reported in the *Cybercrime Judicial Monitor*, it could be observed that, on the one hand, data retention laws in several Member States were annulled by Constitutional Courts in the aftermath of the invalidation of Directive 2006/24/EC. On the other hand, the admissibility of evidence, obtained on the basis of existing data retention laws, has been frequently challenged by the defence, in some cases with success.

Eighteen respondents indicated that, generally speaking, data obtained in contravention of domestic law would not necessarily be considered as inadmissible evidence in court (BE, CZ, DK, DE, EE, IE, ES, FR, HR, LU, HU, NL, AT, PL, LV, SI, FI, SE). In many Member States, this is not directly regulated and thus it is the discretion of the court to decide on the admissibility of the evidence presented. In some Member States, evidence is only excluded in a limited number of circumstances defined by law.

([36]) Appeal Court ruling of 13 May 2024 (case 1-24-1694).
([37]) Judgment of the Irish Supreme Court, *The People (DPP) v Caolan Smyth*, S:AP:IE2022:000110.
([38]) *Cybercrime Judicial Monitor*, https://www.eurojust.europa.eu/cybercrime-judicial-monitor.

A few Member States have introduced **best practices or guidance** to inform law enforcement and judicial authorities on case-law developments, at both the national and the EU level, in relation to data retention and access to data for the purposes of criminal investigation and prosecution. These practical efforts aim, on the one hand, to ensure that data is or can be gathered in a correct manner and, on the other hand, to raise awareness and update prosecutors (with a view to having a unified national point of view), judges and courts about the evolving case-law. Two Member States (BE, FR) disseminate the CJEU and national court rulings amongst prosecutors and judges. One Member State (IE) indicated that updates in this area are routinely included in training, knowledge management and conference programmes for prosecutors. The Court of Cassation in France has also drafted a vade mecum for examining a plea relating to connection data, setting out step by step the reasoning to be applied. In Spain, the prosecution service has recommended the more intensive use of data preservation measures.

4.6. Impact of the CJEU rulings on judicial cooperation in cross-border criminal investigations

From what has been described above, it is clear that the CJEU case-law has had and continues to have a considerable impact at the national level. Legal frameworks on data retention have been annulled, amended or introduced, the availability of data has been impacted and there have been many court rulings in which the admissibility of data as evidence was assessed. It is therefore also important to assess whether, how and to what extent the CJEU case-law has impacted cross-border judicial cooperation in criminal investigations.

Respondents were asked whether the CJEU rulings had an effect on their **ability to provide retained data to foreign authorities** upon their request and/or execute European Investigation Orders (EIOs) or mutual legal assistance requests. Five respondents indicated that less data was available as a result of the lack of retained data, the limitations imposed on the categories of data that can be retained or the short(er) retention periods (CY, IE, RO, SK, SE). Germany also indicated that there is less data available. This unavailability of data is, however, a result of the pre-existing absence of a data retention regime, rather than a consequence of the CJEU rulings ([39]). The unavailability of data consequently also affects authorities' possibility to execute EIOs or mutual legal assistance requests. The remaining respondents indicated that they have not noticed an impact or that they did not have sufficient information available to assess this.

A few respondents (BE, NL, SK) also mentioned that they had encountered issues in relation to the **execution of EIOs sent to other Member States to receive data**. EIOs were not executed due to the lack of, or very limited, data retention regimes. In some cases, service providers have taken this legal vacuum as an opportunity to enforce short retention periods (e.g. a few days), rendering an EIO or even a direct request or freezing order useless. In one Member State, it has occurred that a court refused to issue a national court order, which needs to be provided to the requested country. In a pre-trial stage, only a prosecutor may issue an EIO and the court has no power to validate such an EIO (SK). The remaining respondents indicated that they have not noticed an impact or that they did not have sufficient information available to assess this.

([39]) There has been no mandatory data retention regime in force in Germany since 2008.

These experiences show that cross-border judicial cooperation has been affected, mainly by the unavailability of data. The CJEU case-law has thus indeed impacted authorities' ability to provide retained data to foreign authorities and/or receive retained data from abroad.

5. Main findings

Data retention regimes

- Currently, a few Member States do not have specific legislation on mandatory data retention for law enforcement purposes. Most Member States thus have data retention laws in place.
- Many national data retention legal frameworks in the EU have undergone changes over the past several years as a direct result of the CJEU case-law. In half of the Member States, data retention laws have been amended, or new laws have been introduced, with a view to aligning with the requirements stipulated by the CJEU. A few Member States have not introduced new legislation since the annulment of their data retention law.
- Although many Member States still have data retention laws in place that are not targeted in the sense stipulated by the CJEU, several have introduced legislation over the past several years that is (partially) targeted. The targeting criteria and/or the way in which the targeting is introduced differs among Member States.
- Most of these Member States apply the targeting criterion to the categories of data. Some of them have excluded certain categories (e.g. traffic and location data) as a whole from the data retention obligations. A few Member States have introduced expedited retention (quick-freeze) to oblige service providers to retain data that would otherwise not be allowed to be retained. One Member State has linked the obligation to retain data to geographical areas with certain crime rates. In other Member States, the targeting is focused on the means of communication (e.g. telephone data). In a few Member States, general and indiscriminate retention of data is only allowed for specific categories of data (subscriber data and/or IP addresses) or for specific purposes (threats to national security).
- Member States that have data retention rules in place have defined time limitations within which data can be retained. These data retention periods differ significantly between Member States.
- Several Member States have also amended or introduced new provisions for access to data retained by service providers. These changes were mainly related to the judicial authority that can authorise the access and the limitations as to the seriousness of the investigated crime for which access can be requested. Member States' thresholds as to the minimum imprisonment sentence imposed for 'serious crime' differ.
- Many Member States still indicated that work is ongoing to assess and amend current data retention rules, be it at the level of retention of data or access to such data.

Impact on cross-border investigations and prosecutions

- The unavailability of data is a key issue encountered in evidence collection. This unavailability is sometimes a result of the limitations imposed on the data that can be retained and accessed, sometimes a consequence of the (too) short retention periods or sometimes due to the overall lack of a data retention regime. The possibility to use obtained data as evidence in court is also of relevance.
- In many Member States, the admissibility of evidence, be it collected at the national level or abroad, is challenged in court. Courts regularly need to assess whether retained data can be used as evidence in a criminal case.
- Given the decrease in available data at the domestic level, it can be observed that judicial cooperation is also negatively impacted. In some cases, judicial authorities were not able to provide data to or receive it from foreign authorities due to the unavailability of data.

6. Conclusions and recommendations

Data retention regimes in many Member States have been changed over the past several years or are currently being reviewed in an attempt to bring them in line with the requirements of the CJEU. Member States that have introduced targeted data retention rules and/or amended rules for access to data in their domestic legislation have done so in different ways. Moreover, data retention periods still differ significantly across the EU. This impacts the availability of data for criminal investigation purposes considerably.

Therefore, although some domestic laws may now meet the requirements set by the CJEU, it can be concluded that the varying efforts of Member States have not resulted in a legal framework on data retention in the EU that follows a recognisable or similar pattern.

This legislative disharmony and the unavailability of data impact legal certainty and the effectiveness of criminal proceedings both at the national level and in the context of judicial cooperation in criminal matters.

The e-evidence package has introduced new tools and mechanisms that aim at strengthening international cooperation. A minimum level of certainty and uniformity with regard to the availability of data is, however, required for these tools and mechanisms, and by extension, international cooperation, to be effective. In this context, providing for adequate minimum data retention periods would ensure sufficient time to enable effective criminal investigations.

In light of all the above and according to the information gathered, the development of a common EU framework for data retention for the purpose of criminal investigations and prosecutions seems to be considered by practitioners as a reasonable next step to ensure the efficiency of the criminal justice system.

Annex 1 – Questionnaire

Questionnaire to the EJCN

On the effect of the CJEU Judgements on Data Retention on Member States and Judicial Cooperation

For the sake of this questionnaire, the term 'data retention' applies to non-content data (subscriber information, traffic, location and other transactional data) retained prior to any investigation or court process.

Judgments of the CJEU refers to decisions on data retention (see Cybercrime Judicial Monitor nr. 6)

1. Current legal framework

Was there any new legislation implemented in your country because of the Jurisprudence of the CJEU on data retention from 2018 to 2022?

Please detail/describe in brief the current domestic laws/regulations governing the mandatory retention of electronic/digital data for the purposes of national security, prevention, detection, investigation and prosecution of criminal offences, and access to such retained data by criminal law enforcement authorities.

Please provide the references in your law(s), preferably in English.

2. Scope and safeguards (the principles of proportionality and necessity) on mandatory data retention.

2.1. **General/Mass indiscriminate retention** – Do your domestic laws/regulations on data retention provide for the mass and indiscriminate retention of electronic/digital data?

2.2. **IF NOT, does your legislation:**

2.2.1. stipulate clear and precise rules governing the extent/scope of data retention measures?

2.2.2. detail/describe the circumstances and the conditions in which a data retention measure may be adopted?

2.2.3. require objective evidence which makes it possible to identify a suspect whose data is likely to reveal a link with a criminal activity?

2.2.4. differentiate between categories of i) data (location/traffic), ii) users/subscribers and iii) means of communication (phone/internet) or use other targeting criteria (e.g. geographical) to narrow the scope of data collection ('targeted preventive data retention")?

2.2.5. If **YES** for any of the above, please elaborate, identifying relevant statutory provisions?

3. Safeguards related to **access** to retained data by relevant/competent national authorities.

3.1. **Does your legislation:**

3.1.1. require prior review by a court or an independent administrative authority to grant access to data? If so, please specify which.

3.1.2. detail/prescribe other conditions, substantive and/or procedural, under which competent national authorities can have access to data?

3.1.3. provide for a mechanism for the waiver of such a prior review in the case of validly established urgency?

4. Developing initiatives regarding safeguards (sections 2 and 3)

In circumstances where any of the above safeguards are not currently provided within your domestic legislation, are you aware of any initiatives being undertaken to legislate/provide for such safeguards?

5. Collection and admissibility of evidence.

5.1. Are there circumstances where data retained in contravention of your domestic legislation is admissible as evidence in a criminal trial?

5.2. Has there been any impact of the CJEU rulings in relation to the:

5.2.1. unavailability of data for the purposes of investigation?

5.2.2. discontinuation of ongoing investigations/prosecutions?

5.2.3. admissibility of data retained in contravention of the terms of the judgments of the CJEU?

5.2.4. appeals of convictions based on retained data?

5.3. Please specify any practical solutions/best practices that you might have identified to deal with any of the abovementioned issues.

5.4. Has there been any judgement of a domestic court, which has determined the admissibility of data retained (either before or after 01/01/2018) in contravention to the terms of the of the CJEU jurisprudence?

5.5. In addition to the possible reply to question 4, has there been any impact of the CJEU rulings, by way of amendment of national legislation or administrative policy/instructions on the application of criminal procedural law or are any planned?

22

5.6. Is data retained by electronic service providers legitimately, for their own purposes, admissible as evidence in a criminal trial?

If you have replied **YES** to this question please provide concrete examples in relation to your jurisdiction.

6. Judicial cooperation perspective in cross-border situations

6.1. **Did the CJEU jurisprudence on data retention directly impacted:**

6.1.1. the ability of your authorities to provide retained data as evidence to another Member State?

6.1.2. the ability of your law enforcement authorities to receive, and subsequently present as evidence, retained data from another Member State?

6.1.3 the ability of your judicial authorities to execute LORs or EIOs related to requests to share digital evidence?

6.2. Please detail any examples where the terms of the CJEU judgements affected international cooperation in criminal matters, such as the unavailability of data for the purpose of the investigation.

7. General

Do you anticipate other consequences, are aware of any domestic reports/judgements or have any other comments to make regarding the impact the CJEU judgements on data retention in your investigations?

Example: Impact of new legislation in fundamental rights issues by targeting data retention in certain territorial limits.

Annex 2 – Replies to questionnaire: current legal frameworks on data retention

Member State	Substantive legislation governing data retention	Comments	Procedural regulation governing access by law enforcement agencies
BE	Article 126 Electronic Telecommunications Law	Law of 20 July 2022 on the collection and retention of identification data and metadata in the electronic communications sector and their provision to the authorities following the Constitutional Court ruling of 22 April 2021.	Articles 39quinquies, 46bis, 88bis, 90ter and 90quater Code of Criminal Procedure
BG	Article 251b–i Electronic Communications Act		Articles 159a and 172 Code of Criminal Procedure
CZ	Section 97 Act No 127/2005 Coll., on Electronic Communications	Constitutional Court ruling of 14 May 2019 (data retention rules are constitutionally compliant).	Sections 7b and 88a Act No 141/1961 Coll., Code of Criminal Procedure Sections 68 and 71 Act No 273/2008 Coll., on the Police of the Czech Republic
DK	Sections 786 b–f Administration of Justice Act	The Danish Administration of Justice Act was changed in 2022.	Section 783, cf. Sections 781 and 781a, and Section 806, cf. Sections 804a and b Administration of Justice Act
DE	/	There are currently no legal provisions on mandatory data retention.	
EE	Article §111'1 Electronic Communications Act	The Code of Criminal Procedure was amended in 2022.	§90'1 Code of Criminal Procedure
IE	Communications (Retention of Data) Act 2011 as amended. A consolidated version of the legislation produced by the Irish Law Reform Commission is available here.	The Communications (Retention of Data) (Amendment) Act 2022 amended the Communications (Retention of Data) Act 2011.	Sections 6, 6A-6F and 7, 7A-7D Communications (Retention of Data) Act 2011 as amended

Member State	Substantive legislation governing data retention	Comments	Procedural regulation governing access by law enforcement agencies
EL	Law 3917/2011		Law 5002/2022
ES	Law 23/2007 of 18 October 2007 on the retention of electronic communications and public communication networks data	This law is still in force. Supreme Court rulings of 23 March 2020 (Case No 727/2020) and of 19 October 2022 (Case No 824/22)	Articles 588bis and 588ter Code of Criminal Procedure
FR	Article L34-1 Postal and Electronic Communications Code		Articles 60-1, 60-2, 77-1-1 and 77-1-2, 99-3 and 99-4 Code of Criminal Procedure
HR	Articles 53 and 54 Electronic Communications Act	New provisions of the Electronic Communications Act, 12 July 2022	Article 339a Criminal Procedure Act Article 68 Police Duties and Powers Act
IT	Decree-law No 132 of 30 September 2021 (as enacted and amended by Law No 178 of 23 November 2021)		Sections 123 and 132 Data Protection Code (Decree-law No 132 of 30 September 2021)
CY	Article 4 Law on the Retention of Telecommunication data for the investigation of serious offences – Law 183(I)/2007		
LV	The Electronic Communications Law	On 29 July 2022, a new Electronic Communications Law entered into force in Latvia, which was developed to take over Directive No 2018/1972/EU of the European Parliament and the Council of 11 December 2018 on the establishment of the European Electronic Communications Code measures determined.	Articles 191 and 192 Criminal Procedure Law
LT	Articles 77(2), 78(5), 96(1) and 96(4) Law on Electronic Communications	Law No XIV-635 of 11 November 2021 amended the Law on Electronic Communications	Articles 154(1), 155(1) and 160-1(1) Code of Criminal Procedure
LU	Articles 5, 9 and 10bis Law of 30 May 2005 on the protection of privacy in the electronic communication sector	The special provisions governing surveillance measures for the purpose of national security are laid down by the modified Law of 5 July 2016 on the organisation of the State Intelligence Service.	Articles 48-27 and 61-1 Code of Criminal Procedure

Member State	Substantive legislation governing data retention	Comments	Procedural regulation governing access by law enforcement agencies
HU	Section 159/A Act C of 2003 on electronic communications		Sections 157, 157§2 and 157§10, Section 262(1) Code on Criminal Procedure
MT	Data Protection Act (Chapter 586 of the laws of Malta) Articles 20 and 21 subsidiary legislation 586.01 Processing of Personal Data (Electronic Communications Sector) Regulations		Articles 19 and 22 subsidiary legislation 586.01 Processing of Personal Data (Electronic Communications Sector) Regulations
NL	/	There are currently no legal provisions on mandatory data retention.	
AT	Article §167 Telecommunications Law (TKG)	New data retention law following the Constitutional Court ruling of 27 June 2014.	§76a(2), §134 Z 2b and §137(1) Code of Criminal Procedure
PL	Chapter 4, Article 18 Act of 18 July 2002 on Electronically Supplied Services Articles 180a and 180c Act of 16 July 2004 Telecommunications Law		Chapter 25, Articles 217-219, 236a Act of 6 June 1997 Code of Criminal Procedure
PT	Article 6 Law No 18/2024 (5 February 2024)	In April 2022, the Portuguese Constitutional Court declared Articles 4, 6 and 9 of the Portuguese Data Retention Law unconstitutional (Law 32/2008). Law No 18/2024 (5 February 2024) modified the phrasing of these articles along with the revision of other provisions (Articles 2,7, 15, 16 and 17).	Articles 3(2), 6, 7 and 9(8) of Law No 18/2024 (5 February 2024)
RO	Article 5 Law 506/2004 concerning the processing of personal data and privacy in the electronic communications sector (*processing of data for business purposes*)	There are currently no legal provisions on mandatory data retention.	Article 152 Criminal Procedure Code Article 12 indent 1 Law 506/2004 concerning the processing of personal data and privacy in the electronic communications sector

Member State	Substantive legislation governing data retention	Comments	Procedural regulation governing access by law enforcement agencies
SI	Electronic Communications Act (ZEKom-1)	There are currently no legal provisions on mandatory data retention.	Articles 149b and 149c of the Criminal Procedure Act
SK	Section 112 §2 and §3, Section 117 §6 Act No 452/2021 Coll. on electronic communications		Section 116 Code of Criminal Procedure
FI	Section 157 (1003/2018) Act on Electronic Communications Services (917/2014)		Chapter 10, Section 6 Coercive Measures Act (806/2011)
SE	Chapter 9, Sections 19 and 22 Electronic Communications Act (2022:482)	After the Tele2 judgment, the Swedish legislation was reviewed. A new Electronic Communications Act (2022:482) entered into force on 3 June 2022.	Part 2, Chapter 27, Section 19 Swedish Code of Judicial Procedure Articles 1-3 Act (2012:278) on Law Enforcement Agencies Access to Information Regarding Electronic Communication

Member State country codes

BE	Belgium
BG	Bulgaria
CZ	Czechia
DK	Denmark
DE	Germany
EE	Estonia
IE	Ireland
EL	Greece
ES	Spain
FR	France
HR	Croatia
IT	Italy
CY	Cyprus
LV	Latvia
LT	Lithuania
LU	Luxembourg
HU	Hungary
MT	Malta
NL	Netherlands
AT	Austria
PL	Poland
PT	Portugal
RO	Romania
SI	Slovenia
SK	Slovakia
FI	Finland
SE	Sweden

Eurojust, Johan de Wittlaan 9, 2517 JR The Hague, The Netherlands
www.eurojust.europa.eu • info@eurojust.europa.eu • +31 70 412 5000
Follow Eurojust on X, LinkedIn and YouTube @Eurojust

Catalogue number: QP-01-24-001-EN-N • ISBN: 978-92-9404-316-0 • DOI: 10.2812/2621651

Eurojust is an agency of the European Union