Council of the European Union

Brussels, 6 November 2017
(OR. en)

10098/17

LIMITE

JAI 584
COPEN 195
DAPIX 228
ENFOPOL 296
CYBER 94
EUROJUST 91
CT 119

COVER NOTE

From:	EUROJUST
To:	Delegations
Subject:	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 - Report

Delegations will find attached a Report of Eurojust on 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.

ANNEX

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

EUROJUST LIMITED – The distribution of this document is strictly limited to:

- Officials of the Secretariat General of the Council of the European Union and of the European Commission;
- Officials of Member States ministries and permanent representations responsible for justice and home affairs, including delegates to the meetings of the Council of the European Union and its preparatory meetings;
- Members of the Consultative Forum
- Post holders of Europol;
- Members and officials of the European Parliament;
- Members of the European Judicial Cybercrime Network.

Please do not distribute to recipients other than those mentionned above.

Table of Contents

1.Purpose

The College of Eurojust initiated a project designed to assess the impact on judicial cooperation in criminal matters within the European Union of the judgement of the Court of Justice of the European Union (CJEU) in Joined Cases C-203/15 and C-698/15[1] (Tele2 and Watson).

As questions relating to general/mass indiscriminate retention of traffic and location data, the safeguards appropriate to such retention schemes and the control of access to such data by law enforcement agencies are by nature both legal and technical, and often best assessed by practitioners, the assistance of the European Judicial Cybercrime Network (EJCN)[2] was deemed appropriate.

To that end, a detailed questionnaire was sent to the EJCN. Eurojust would like to express its appreciation to the Board of the EJCN, and all its members, for the wholehearted and expeditious manner in which this project was supported.

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

This report is designed to provide practitioners' views on the matter and serve as an experience-based contribution to the assessment of the ongoing situation.

2.Methodology

As mentioned, a detailed questionnaire was drafted for the purpose of this project. The questionnaire was sent to EJCN members in March 2017 (*see* Annex 1). Replies were received from both 'England and Wales' and Scotland, as they are both represented in the EJCN. These replies are thus counted separately in this report. Next to replies from the Member States, replies from Norway and Switzerland were also received and incorporated. In total, 28 replies were received and analysed.

[1] Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others.

[2] 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.

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 Internet Service Providers (ISPs).

In one country (DE), the legislation governing data retention was adopted in 2015, but the provision on data retention will only enter into force in July 2017. For the purpose of this exercise, this country has been treated as having legislation in force. In another country (SE), the existing rules on mandatory retention (which provide for mass and indiscriminate retention) are no longer being applied. Again, for the purpose of this exercise, this country is treated as having such legislation.

More generally, the summary of the replies may not entirely reflect the complexity of each of the national legal systems, as the full context was not always given, due to the objective of the project and focus of some of the questions. Moreover, questions might have been interpreted differently depending on the legislative framework in each country. In this regard, additions by the National Desks at Eurojust were incorporated in the report for the sake of completeness or further clarification. Nonetheless, the report provides a wealth of information as to the legal regimes in place and complements previous initiatives taken by Eurojust in this area.

As only six months have elapsed since the CJEU judgement was rendered, the actual impact of the judgement may not yet be fully apparent. Nonetheless, in light of the developing political landscape, Eurojust determined that this research may still provide significant benefit.

3.Background information

Following the CJEU judgement in Joined Cases C‑ 293/12 and C‑ 594/12 (Digital Rights Ireland) invalidating Directive 2006/24/EC, Eurojust conducted an analysis of EU Member States' legislation and current challenges on data retention. This analysis has been published as a Council document[3]. The matter was also the subject of a dedicated workshop in the framework of the meeting of the Consultative Forum of Prosecutors General on 10-11 December 2015.

The analysis showed that:

> '*the fragmented regulation in place undermines criminal investigations and prosecutions as well as judicial cooperation in the fight against serious crime. […] there [have] been a significant number of challenges to the admissibility of evidence in criminal proceedings in approximately a year from the judgement […]. In addition, several states currently have no defined legal data retention framework upon which law enforcement and judicial authorities may efficiently and rapidly operate.*'

The Consultative Forum concluded that *'[a] European common framework to harmonise retention of and access to data is necessary'.*

[3] *Eurojust's analysis of EU Member States' legal framework and current challenges on data retention*, published as Council document ST 13085/15, *Limité.*

Such conclusion echoed the CJEU ruling in the Digital Rights Ireland judgement[4], which acknowledged that '*the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest*' and that '*such […] EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question*'.
The ruling of the CJEU of 21 December 2016 provides a sort of complement to the above.

The CJEU finds that EU law **precludes a general and indiscriminate retention of traffic data and location data**. The Court, however, provides that Member States are free to regulate data retention, in a targeted manner, **for the purpose of fighting serious crime**. Such retention should, however, 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 the national authorities to the retained data must be subject to conditions, including **prior review by an independent authority** and the data being retained within the European Union.

Another highlight of the judgement stipulates that **national legislation must be clear and precise and must provide sufficient guarantees** for the protection of data against risks of misuse. The legislation must indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, **thereby ensuring that the scope of that measure is, in practice, actually limited to what is strictly necessary**. Such legislation must be based on **objective evidence,** which makes identification of the persons whose data is likely to reveal a link with serious criminal offences possible, thus contributing to fighting serious crime or to preventing a serious risk to public security.

4.Analysis of the replies to the questionnaire

4.1.Mandatory data retention: legislation

All respondents provided the reference to their domestic legislation governing data retention for law enforcement purposes in their countries.

The vast majority regulate the matter in their electronic telecommunication laws and/or penal/procedure codes. Six replies indicated that no such law regulates the matter and thus that they rely on obligations to retain data for business/commercial purposes.

The compilation of replies can be found in *Annex 2*.

[4] In Case C-293/12 of 8 April 2014 (Digital Rights Ireland Ltd), the CJEU invalidated Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

4.2.Mandatory data retention: scope

To determine whether data retention provisions in the countries are of a general nature or targeted in the sense of the CJEU ruling, an assessment was made to determine whether they 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[5], or the 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 that their data retention regime is targeted by virtue of the limitations set with regard to retention periods and/or reason for the data retention. For the purpose of this analysis, we have therefore interpreted the answers on the basis of the content of the legislation, rather than the indicated reply.

As a result, three types of legal regimes emerge from the replies:

- The vast majority of the countries do not have targeted data retention rules within the categories of location/traffic data, users/subscribers, and means of communication (internet/telephone).

- One country (DE) reported that it excludes some targeted users/subscribers from the retention obligation in the legislation that is to come into force in July 2017, as is the situation for '[…] data pertaining to telephone connections to and from persons, public authorities or organisations in the social or the church domain that offer anonymous counselling', as well as '[…] data about websites being visited or regarding e-mail'. This legislative model approaches the targeting criterion detailed in the CJEU judgement, but differs in so far as it stipulates data that may not be retained from a particular category of users/subscribers as opposed to targeting specific data to be retained.

- Finally, some countries (AT, NL, RO, SI, SK) reported that they do not have data retention laws for law enforcement purposes only, following the annulment of their previous laws by their constitutional/high courts in accordance with the DRD judgement[6]. As a result, they all reported using data collected by private operators for business or/and commercial purposes. The questionnaire did not address the retention scheme in this context.

It can be concluded that none of the countries have national legislation that obliges the targeted retention of data linked to specific persons or geographical locations.

Practically all countries have provisions on mandatory time limitations for data retention. *See* Annex 3.

Some respondents highlighted that the necessary safeguards are contained in the limitations placed on **access to the data** by the law enforcement agencies rather than the retention scheme as such.

[5] *See* Annex 3 for a summary of the retention periods.

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

4.3.1. Prior review by a court or an independent body

The vast majority of the respondents (23) outline that a judicial review is required, prior to or after the request for access has been made.

In most countries, prior authorisation/judicial review is required before access is granted to law enforcement (LEA). This review takes the form of a **court order/order of an investigative judge**, or an order by a **prosecutor**. In some specific circumstances, judicial police or similar authorities can have direct access to such data, for a limited period of time, without prior review by a court. In two countries, the required judicial review depends on either the stage of the proceedings (LV) or the nature of the data requested (BE): distinction is made between subscriber data, for which a prior production order from a prosecutor is required, and traffic data, for which a prior production order from an investigating judge is required, and in exceptional cases (such as terrorism) by a prosecutor.

In some countries, review *a posteriori* is foreseen. Four countries report that access is granted primarily to authorities belonging to the executive with no specific reference to it being 'independent', but with some degree of judicial supervision. Such is the case in the legal systems in one Member State (UK, including Scotland), in which 'relevant public authorities', all affiliated with the executive branch, have access to data, provided that the decision to give notice has been approved by a Judicial Commissioner (appointed by the Prime Minister). One country (IE) entrusts the determination of access to data to a superior officer of the law enforcement agency, under the general supervision of the judiciary (tasked to oversee the proper application of the law based on a report submitted to the Prime Minister). One country (PL) responded that access lies primarily with the law enforcement agencies, under the general supervision of a court to which the LEA send reports twice a year.

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

The replies suggest that access is granted depending on the **nature of the crime/seriousness of the act**, or is based on the **minimum threshold of penalties** foreseen, which range from one to six years in the different countries (BE, CH, DE, HR, NO, PT, RO, SK).

The court order/request issued needs to be, the latter is **motivated by and/or takes due account of principles such as necessity, proportionality, subsidiarity and/or legality**. In one case (DK), the conditions vary depending on the type of data sought, and access to retained traffic data may only be pursued if the investigation concerns an offence punishable by imprisonment of no less than six years or other specific and serious offences. The subscriber and location data can be accessed in principle in all types of criminal cases if the courts find that they are proportionate on the basis of a concrete evaluation of the conditions of the individual case.

Actual access is subject to safeguards in at least one country (PT) and must be authorised by a senior operation officer who is independent from the operation concerned in one country (UK), and/or has a high-ranking position (IE). In at least two other countries (BE, PL), access is subject to internal logs in dedicated repositories and specific rules for ISPs protect unauthorised access.

Time limitation in terms of access by law enforcement is mentioned by one country (SK) as being six months, with a possibility of extension. In another country (BE), time limitation in terms of access is quite detailed and complex, depending on the type of data requested, the nature of the crime and the severity of the penalty. As a result, in some cases no access is allowed, or time limitations for access can be six, nine or twelve months.

Two countries (BE and DE) reported restrictions regarding the access to **data related to professions enjoying privileged communications** (e.g.: lawyers, journalists, doctors).

One country mentioned that the data subject needs to be notified of the request made to the ISP in certain circumstances.

4.3.3. Requirement of prior review by a court or an independent administrative authority in emergency situations

Of the sixteen positive replies, eight respondents reported the existence of a specific procedure in the event of emergency. In the vast majority of these cases, a member of the judiciary (judge or prosecutor) is involved.

In some countries, the required review is more flexible in emergency situations. Some countries allow for an oral request by the competent authority, provided confirmation in writing follows (BE, HR, IE, NO). One country (DK) entrusts the police or the intelligence service to proceed, provided that a court review is conducted within 24 hours.

One country (UK, including Scotland) reports that in case of emergency, the regular procedure consisting of approval by an accredited individual trained to facilitate lawful acquisition of communications data and effective cooperation between a public authority and ISPs does not apply.

In three countries (BG, CZ, SE), the police are granted authority to request direct access to data in pre-defined circumstances, including in the field of terrorism.

4.4. Developing initiatives regarding legal changes to legislation

A review/assessment is currently ongoing in eight countries (AT, BE, DK, EL, IE, LV, SE, UK) and working groups of an inter-ministerial nature have been set up in two countries (MT, SK).

Amendments are in the drafting stage in three countries (CH, EE, NO), and legislative changes are at an advanced stage in two countries (NL, SI). Substantive legislative changes being contemplated or drafted primarily concern:

- the introduction of a review mechanism in case of emergency (MT, SE),
- the introduction of the notion of targeted retention and quick freeze (AT),
- the distinction between various categories of providers concerning all main categories of data, access to retained data to be subject to prior authorisation from the investigative judge and public prosecutor in accordance with the principles of proportionality and necessity (NL),
- in one country (SI), a series of amendments to ensure, *inter alia*, that requests for access concern serious crimes only; the possibility for LEA to place an oral order in the event of emergency; the possibility for operators and service providers to appeal the order from police or prosecutors to the investigative judge, and
- the extended scope of providers to which the mandatory data retention will apply (CH).

Six countries responded that no initiative is ongoing (CZ, ES, FI, IT, PL, PT), but two countries (ES, FI) suggested that a review may be conducted in the future.

4.5. Collection and admissibility of evidence

Respondents were asked to identify any immediate impact of the CJEU judgement, particularly in relation to the collection and admissibility of evidence.

Four countries (NL, PL, SE, SK) replied that they had already encountered issues with regard to the **availability of data** from ISPs, simply due to the lack of a data retention obligation and/or a lack of clarity, since the CJEU ruling, concerning the type of data that should be stored or provided by ISPs. Unavailability of data also impacts on the possibility to provide data to other countries on the basis of an MLA request.

Most countries replied that requesting access to and using data stored for business purposes by ISPs is possible for the purpose of criminal investigations. If such data is available from ISPs, law enforcement authorities could thus make use of the data, which possibly provides a practical solution to the abovementioned issue of unavailability of data.

Two countries (IE, NL) reported issues in relation to possible **discontinuation of cases**. Others pointed out that this situation might indeed occur in investigations conducted in their countries in the future.

The impact of the CJEU rulings has up to now mostly been noticeable in the context of assessing the **admissibility of evidence** in court. Five countries (BE, EE, ES, FR, IE) have reported on court rulings (first instance, appellate court, Supreme Court or appeal of convictions) in which the gathered evidence in a case was or is being evaluated by the court. So far, the evidence was found to be admissible in all of these court cases, although one case is still pending and a decision by an appellate court in Ireland has not yet been taken. In two countries (BE, IE), evidence would only be excluded in a limited number of circumstances. The evidence under scrutiny in the particular cases was rendered admissible. In one country (ES), the court ruled that the law contained sufficient safeguards and controls, minimising the risk of violation of the right to privacy and data protection laws. In one country (EE), the Supreme Court ruled that the existing laws, containing provisions on the gathering and use of information from ISPs in criminal proceedings, were constitutional.

Respondents were also asked if data obtained in contravention of domestic legislation could still be considered admissible in court. Nine countries responded that such evidence would be considered inadmissible. Moreover, in one country (PT), illegally obtaining and accessing data is punishable with two years' imprisonment. Although the use of illegally obtained data by authorities is not permitted in two more countries (CZ, HU), the use of data obtained by private individuals is permitted. Thirteen respondents (BE, DK, EE, EL, ES, IE, LV, MT, NO, RO, SE, UK, including Scotland) replied that, although evidence would be obtained illegally, it could still be considered admissible in court. In many countries, the court has discretion to decide on the admissibility of the evidence presented. In some countries, evidence is only excluded in a limited number of circumstances defined by law. For example, in one country (BE), illegally obtained evidence will only be rendered void if: (1) the violation of the procedural rule is explicitly sanctioned with annulment, (2) the irregular act has affected the reliability of the evidence, or (3) the use of the illegally obtained evidence would violate the right to a fair trial. In another country (ES), the illegally obtained evidence would be admissible in *bona fide* cases or cases in which the defendant pleads guilty or confesses to the crime.

Fifteen respondents replied that they are **not aware yet of any immediate impact** on the collection and/or admissibility of data gathered by law enforcement from ISPs. As the majority of the respondents did not identify some or any of the abovementioned consequences, determining and assessing the full extent of the impact of the latest CJEU ruling is probably premature.

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

The effect of the CJEU ruling on the availability and admissibility of evidence gathered from ISPs is or will consequently also be noticeable in the area of cross-border judicial cooperation in criminal investigations. Both the ability of authorities to provide data to other countries upon their request as well as the possibility to receive and use data gathered from other countries, could potentially be affected by the CJEU ruling.

Although all respondents, except for two, replied that they did not (yet) encounter any negative impact in the area of judicial cooperation, many did express concerns for future cooperation, particularly in relation to availability of data. In one country (SE), due to the fact that data is currently not retained, gathering the requested data has indeed been impossible. Another Member State (BE) encountered problems with some countries having very short data retention periods, which resulted in the unexpected loss of e-evidence. Many respondents agreed that, if data is not available due to lack of data retention obligations, executing MLA requests will be impossible, and judicial cooperation as a whole will be adversely affected.

Some countries mentioned that their laws on data retention are still in force or being applied, whether or not they are being evaluated in light of the CJEU ruling. Others stated that evidence gathered abroad is presumed to be collected in accordance with the law of that country, and therefore could be used in their country and would be admissible. However, for countries not applying this concept, hypothetically, if data is requested from another country and it would be obtained in contravention of the CJEU rulings, one would have to refer to the rules on admissibility of evidence to assess whether the data could be received and used in subsequent domestic investigations and proceedings (*see* above). This means that, although the data could still be received through judicial cooperation, its use might be questionable.

Thus, cross-border judicial cooperation will be affected in the future, mainly because of unavailability of data, but probably also with respect to the (im)possibility to use data received from other countries, which, following the ruling of the CJEU, are in an unclear situation as to the legality of data obtained.

4.7. Respondents' remarks in relation to the CJEU ruling

Respondents were asked if they had any further comments in relation to the ruling. Their views and remarks are reflected below.

Respondents have expressed great concern about the impact of the CJEU ruling(s) on criminal investigations and proceedings. Retention of data is an essential part of the investigative process. Police and judicial authorities usually rely heavily on communications data to successfully proceed with their casework.

In the absence of any data retention rules or in the current context, in the aftermath of the CJEU ruling, the main negative result will be the unavailability of data, because it is not stored by ISPs and/or disclosed to law enforcement authorities upon request. As a consequence, the decision on which data will be stored by ISPs and provided to authorities is left to the discretion of the ISPs themselves. Moreover, each ISP can apply a different policy. In addition, the level of cooperation from ISPs with law enforcement authorities differs, or, in some cases, has already decreased. Furthermore, if countries need to rely solely on data stored by ISPs for business purposes, the available data might be too limited.

EU Member States will have less data available (retained and/or accessed) to them, and they can probably obtain or provide less evidence from each other than from third countries.

With regard to some of the conditions laid down in the ruling of the court, namely the restriction of the retention to specified data and to specified targets, some respondents argued that it is impossible to determine in advance the individuals who will commit crimes and thus the data that will need to be preserved. Moreover, one might argue that using data stored indiscriminately for all citizens, simply because of the fact that it was retained in a non-targeted, non-discriminatory way, is more acceptable. The retained data can then be used as evidence of a crime because they were preserved indiscriminately. Targeting specific categories of persons, e.g. persons living in a particular geographical location, could moreover result in targeted investigations, which could eventually also be considered discriminatory.

Therefore, respondents stated that focusing on safeguards for storage, disclosure and access to data seems more feasible from a practical point of view than limiting or targeting specific categories of data to be retained. A reasonable assertion to make is that the privacy of individuals to which the data refers should not be impacted disproportionately if sufficient safeguards are put in place regarding the specific purpose for which the data is held, lawful disclosure and stringent judicial oversight. Privacy rights are outweighed by the rights of society in general to public safety, to life, to freedom from harm, damage or injury and to justice.

Reference was made to the considerations in the ECHR Judgement in the case of *K.U. v. Finland, n° 2872/02*, of 2 December 2008. The Court states that the principle of practical effectiveness of protection and its implication to require practical effectiveness of investigations also covers electronic evidence and information necessary to identify the perpetrator of an alleged offence. Legislators are required to provide access to communication data, and governments should ensure the conditions for successful criminal investigations in cases in which essential values and elements of private life are at risk.

Reference was also made to the condition laid down by the CJEU on the seriousness of the offence (and therefore the limited categories of offences). This criterion would thus need to be applied to access to data in criminal investigations, whereas it does not apply to access to data kept for business purposes.

The obligatory storage of data by ISPs on EU territory was also touched upon.

5. Main findings based on the replies to the questionnaire

Data retention regimes:

i. While some countries do not have specific legislation on mandatory data retention for law enforcement purposes, the vast majority of countries do.

ii. No country appears to have legislation containing all the specific targeting criteria stipulated by the CJEU, i.e. requiring data retention to be permitted only in a targeted manner for the purpose of fighting serious crime, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the duration of retention. One country's legislation does exclude some targeted users/subscribers from the retention obligation.

iii. All countries provide for some form of limitation of access, which seeks to balance the need for access in the interest of criminal investigations and prosecutions with the rights of citizens.

iv. Some respondents expressed the view that this necessary balance is already guaranteed by the limitations placed on access to the data by LEA and thus limitations should not concern the scope of the mandatory data retention rules as such.

v. Most countries that have mandatory data retention rules for law enforcement purposes have defined time limitations within which data can be retained. They vary from several weeks to up to three years.

Potential impact on investigations and prosecutions:

vi. The unavailability of data (not stored or not provided by ISPs) is one of the main concerns expressed by respondents in relation to evidence collection. Discontinuation of ongoing investigations and prosecutions is foreseen, as well as challenges to the admissibility of evidence at a later stage.

vii. Almost all respondents replied that they did not yet encounter any negative impact in the area of judicial cooperation. Many did express concerns for future cooperation, particularly in relation to availability of data as well as admissibility of data gathered in a foreign country.

viii. Many respondents remain concerned about the likely effect of this judgement, as they perceive data retention (even general and indiscriminate) as an essential investigative/prosecutorial tool in the fight against serious crime and terrorism. Identifying or targeting specific electronic data that may ultimately become probative evidence in a prosecution, seems difficult.

ix. Aware of the situation, more than half of the countries indicate that work is in progress to adjust/assess the legal regimes in place against the CJEU judgement.

6. Conclusions and recommendations

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. With so many countries currently reviewing their domestic legislation to design data retention regimes that meet the requirements of the judgement, and so many variables at play, the potential for continued legislative disharmony within in the European Union is considerable.

In this light, consideration of the development of a common understanding of the requirements resulting from the CJEU judgement, at an EU level, seems urgently required. It should thereafter be considered whether a common framework for data retention for the purpose of preventing and fighting crime would be beneficial.

The current state of play requires further monitoring of the legislative developments and the potential impact of the judgement in the months and years to come, both on a national level and in the area of judicial cooperation within the EU in criminal matters.

Annex 1 – Questionnaire

Questionnaire to the EJCN

On the effect of the CJEU Judgement on Data Retention (21/12/16) 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.

1.	Current legal framework

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 immediate impact of the ruling 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 judgement 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 21/12/2016) in contravention to the terms of the judgement of the CJEU?

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

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

6. Judicial cooperation perspective in cross-border situations

6.1. **Does the judgement directly impact on:**

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?

6.2. Please detail any examples where the terms of the judgement has already effected 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 judgement of the CJEU may have on your work?

Annex 2 – Replies to questionnaire, current legal framework

Country	Substantive legislation governing data retention	Comments	Procedural regulation governing access by LEA
AT	Legislation on data retention was invalidated as a result of the CJEU judgement of 2014	Providers can retain data for billing purposes only	--
BE	Electronic Telecommunications Act, 13th June 2005	The law was amended by the Statute of 29th May 2016 concerning the collection and retention of data in the electronic communications sector	Articles 46bis and 88bis of the Belgian Code of Criminal Procedure
BG	Electronic Communication Act (New, SG No. 24/2015 effective 31.03.2015), Art. 251b, d, h, i.		Penal Procedure Code (New, SG No. 24/2015, effective 31.03.2015), Art. 159a and 172
CH	Federal Act on Postal and Telecommunications Surveillance and its regulation (BÜPF and VÜPF), Art. 15 par. 3		Art 273 Criminal Procedure Code (StPO)
CZ	Act on Electronic Communications (Act No. 127/2005 Coll.)		Act No. 141/1963 Coll., Code of Criminal Procedure, Act No. 273/2008 Coll., on the Police of the Czech Republic, Act No. 154/1994 Coll., on the Security Information Service, Act No. 289/2005 Coll., on Military Intelligence, and Act No. 15/1998 Coll., on the supervision in the field of capital markets.
DE	Telecommunications Act, Art. 113b	The law was adopted in December 2015 and will enter into force in July 2017 concerning the provisions governing retention. As a consequence, **for the time being,** no mandatory retention of data. Access to Law enforcement agencies is therefore granted for data retained by companies for business purposes. In the (to be applicable) law, the obligation to retain certain categories of data according to Section 113b Telecommunications Act applies generally insofar as it does not require a certain trigger or occasion for the retention.	--
DK	Danish Administration of Justice Act Executive Order no. 988 of 28 September 2006 on the		Danish Administration of Justice Act, Sections 781-784, 788, 804 (1), 806 (2)

Country	Substantive legislation governing data retention	Comments	Procedural regulation governing access by LEA
	retention and storage of traffic data by providers of electronic communications networks and electronic communications services, amended by Executive Order No. 660 of 19 June 2014		
EE	Electronic Communications Act	Art. 111-1	Code of Criminal Procedure, Art. 90-1
EL	Law 3917/2011 *on Retention of data generated or processed in connection with the provision of electronic communications services or of public communications networks and publicly available services, using surveillance systems to receive or record audio or video in public areas and related provisions*		
ES	Law on the retention of electronic communications and public communication networks data, Law 25/2007 of 18 October 2007.		Criminal Code, Art. 588 ter j), m) and g)
FI	Information Society Code 917/2014, subsection 3 and 4		Information Society Code 917/2014, Section 158
FR	Postal and Electronic Communications Code, Art. L34-1, CPCE Article 6 II of the Law *pour la confiance dans l'économie numérique* (21 June 2004) and its implementing Decree No 2011-219 of 25 February 2011 on the conservation and the provision of data aims at identifying anyone who has contributed to the creation of online content.	Article R 10-13 of the CPCE (introduced by decree n° 2006-358 of 24 March 2006) has strengthened the previous provision as to retention, by the operators, of subscriber, traffic and localisation data and is now mandatory for one year. Article R10-14 of the CPCE provides for the possibility for telecommunication operators to retain certain traffic data for a period not exceeding one year for their billing operations.	Code of Criminal Procedure: Articles 60-1, 77-1-1 and 99-3.
HR	Electronic Communications Act (Official Gazette No. 73/2008, No. 90/11, No. 133/12, No. 80/13, No. 71/14)		Criminal Procedure Act (Official Gazette No. 152/08, No. 76/09, No. 80/11, No. 91/12, No. 143/12, No. 56/13, No. 145713, No. 152/14); Police Duties and Powers Act (Official Gazette No. 76/08, No. 92/14).
HU	Electronic Communications Act, Act 100 of 2003, Art. 159/A Act 112 of 2011	The Hungarian legislation prescribes the general retention of data without differentiating between the severity of the crimes committed or by any other criteria. No prescription of any judicial or prosecutorial consent before the request; the investigating authorities can send them directly to the providers. Petty crimes are, however, excluded from such request and the request should be limited to the information	Act 19 of 1998, Criminal Procedure Act, Art. 71 paragraph 3 and Art. 178

Country	Substantive legislation governing data retention	Comments	Procedural regulation governing access by LEA
		indispensable to serve the purpose.	
IE	The Communications (Retention of Data) Act 2011, Section 3	The e-Privacy Regulations 2011 (S.I. 336 of 2011) deal with data protection for phone, e-mail, SMS and Internet use	The Communications (Retention of Data) Act 2011, Section 6
IT	Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003	Section 123	Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003, Art. 132
LV	Electronic Communications Law, Section 1, Art. 44 and Section 19, Art. 1		Electronic Communications Law, Section 71
MT	Subsidiary Legislation 440.01, Processing of Personal Data (Electronic Communications Sector) Regulations		Subsidiary Legislation 440.01, Processing of Personal Data (Electronic Communications Sector) Regulations
NL	Dutch Communications Act	Previous legislation (*Staatblad* 2009, 333) on data retention invalidated as a result of the CJEU judgement of 2014. Law enforcement is now dependent on the data that the service providers store for their own business purposes and the length of time that providers store this data. Data that is stored by the service provider can be legally obtained and used by the prosecution	Code of Criminal Procedure
NO	Electronic Communications Act, No. 83 of 04 July 2003	Section 2-9. Regarding duty of confidentiality, and, specifically, subsections three and four.	The Criminal Procedure Act, Chapter 16 d, regarding lawful end-point interception, Section 216o.
PL	Data retention is governed within each specific regulation of public service act: Police Act of 6 April 1990, Border Guard Service Act of 12 October 1990, National Tax Administration Act of 16 November 2016, Military Police Act of 24 August 2001, Internal Security Agency Act of 24 May 2002, Military Counterintelligence Service Act of 9 June 2006, Central Anti-Corruption Bureau Act of 9 June 2006. The specification of data and the type of information to be retained can be found in different legislations: Act of 23 November 2012 – Postal Law, Act of 16 July 2004 – Telecommunications Law and Act of 18 July 2002 – Provision of Electronic Services.	These public services have the right to retain non-content data for the purpose of preventing or detecting criminal offences, saving human life or health, and during search and rescue operations.	The 'data retention' was set by amending the specific laws - Act of 15 January 2016, Polish Journal of Laws 2016 no. 147
PT	Law 32/2008 of 17th July		Law 32/2008 of 17th July
RO	Law 506/2004 concerning the processing of personal data	Previous legislation 82/2012 on data retention	Criminal Procedure Code, Art. 152 and 139

Country	Substantive legislation governing data retention	Comments	Procedural regulation governing access by LEA
	and privacy in the electronic communications sector, Art. 5 (traffic data)	invalidated as a result of the CJEU judgement of 2014. The providers are under no obligation to retain traffic and location data, but, as long as the data is available to them, they could be obliged to transmit it, based on a judge's authorisation	Law 506/2004 concerning the processing of personal data and privacy in the electronic communications sector, Art 12
SE	Law on electronic communications (2003:389) Regulation on electronic communications (2003:396)	As a result of the CJEU judgement regarding the Swedish law on data retention, no rules exist on mandatory retention in Sweden, although the law has not been changed yet.	Law on electronic communications (2003:389) Regulation on electronic communications (2003:396) Law on gathering of data relating to electronic communications as part of intelligence-gathering by law enforcement authorities (2012:278) Code of Judicial Procedure
SK	Act No. 351/2011 Coll. as amended		Article 116 of the Code of Criminal Procedure (Act No. 301/2005 Coll., as amended). Art. 116 para 1 of the Criminal Code
SL	The Electronic Communications Act, Official Gazette RS No. 109/12 (partially abrogated, notably re. Art. 162 to 169)	The provisions governing data retention were declared unconstitutional as of 3 July 2014. As a result, no specific retention obligation	Criminal Procedure Act, Art. 149 b (re. traffic data) The Electronic Communications Act, Art. 153

Country	Substantive legislation governing data retention	Comments	Procedural regulation governing access by LEA
UK, including legal regimes in England and Wales and Scotland	Investigatory Powers Act 2016, IPA, Part 4		Regulation of Investigatory Powers Act 2000 In England and Wales, the relevant sections of RIPA relating to the acquisition and disclosure of communications data will be replaced by Part I IPA when those provisions are commenced (Investigatory Powers Act 2016, Part 3)

Annex 3 - Summary of the main findings related to legislation

Replies	Data retention periods (for law enforcement or business/ commercial purposes) (typically running as of the date of the communication or at the end of the subscriber's contract)	Review or legislative changes in progress
BE[7]	12 months	Review ongoing
CH	--	Legislative changes in drafting
CZ	6 months	No
DE	4 to 10 weeks in the new law	A new law was adopted in December 2015, bur the provisions regulating retention will enter into force in July 2017. Until that time, DE has recourse to retention for billing purposes
EE	12 months	Legislative changes in drafting
ES	12 months	No
EL	--	Review ongoing
DK	12 months	Review ongoing
HR	--	--
HU	6 to 12 months	Assessment ongoing
FI	6 to 12 months	No
FR	12 months	No
IE	12 to 24 months	Review ongoing
LV	18 months	Review ongoing
MT	6 to 12 months	Review ongoing
IT	24 months	No
PL	--	No
PT	12 months	No
SE	6 months	Review ongoing (the law is said to be in force, but not being applied)
UK[8]	12 months	Review ongoing
AT	--*	Review ongoing
NL	--*	Legislative changes in drafting
NO	3 months*	Legislative changes in drafting
RO	Up to 36 months*	--
SI	--*	Legislative changes in drafting
SK	-- *[9]	Review ongoing

[7] BE indicated that within the general retention period, access by law enforcement agencies varies from no access to 6, 9 or 12 months.
[8] Including legal regimes in Scotland and England and Wales
[9] SK indicated that consent can be granted for a period no longer than six months, during which time the information is retained and provided; this period may be prolonged, but each time for not more than six months.

Legend:	Countries with no data retention laws, rely on data collected for business purpose of operators
	[*]: While data retained for **billing purposes** are generally time limited, market research or sales activities and data retained for delivering **services with 'added value'** are retained on an opt-in basis and their retention period may be significantly different