



*Consultative Forum
of Prosecutors General and
Directors of Public Prosecutions
of the Member States of the European Union*



**WORKSHOP ON *DATA RETENTION IN THE FIGHT AGAINST
SERIOUS CRIME: THE WAY FORWARD***

AND

**10TH MEETING OF THE CONSULTATIVE FORUM OF PROSECUTORS
GENERAL AND DIRECTORS OF PUBLIC PROSECUTIONS OF THE
MEMBER STATES OF THE EUROPEAN UNION**

THE HAGUE, 10-11 DECEMBER 2015

REPORT AND CONCLUSIONS

WORKSHOP ON
DATA RETENTION IN THE FIGHT AGAINST SERIOUS CRIME: THE WAY FORWARD

AND

10TH MEETING OF THE CONSULTATIVE FORUM
OF PROSECUTORS GENERAL AND DIRECTORS OF PUBLIC PROSECUTIONS
OF THE MEMBER STATES OF THE EUROPEAN UNION

THE HAGUE, 10-11 DECEMBER 2015

REPORT AND CONCLUSIONS

Introduction

The Workshop on *Data Retention in the Fight Against Serious Crime: The Way Forward* and the 10th meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union (Consultative Forum *or* Forum) were organised in The Hague on 10 and 11 December 2015 by the Luxembourg Presidency and Eurojust.

The Workshop permitted the sharing of views among prosecuting authorities on the practical and legal consequences of the annulment of the 2006 Data Retention Directive (DRD) by the Court of Justice of the European Union (CJEU) in its decision in *Digital Rights Ireland Ltd (C-293/12)*. Members of the Consultative Forum, other experts from the Member States, members of the College of Eurojust and representatives of the EU institutions actively participated in the four working groups set up to facilitate discussion. The following day, the outcomes of the working groups were presented to the Consultative Forum.

At the Forum meeting, Forum members discussed and reached conclusions on the following three main topics:

- Data retention (Session I)
- Terrorism (Session II)
- Illegal immigrant smuggling (Session III)

The Forum also discussed its future working methodologies (Session IV).

Workshop on Data Retention (10 December)

Following the welcoming of participants by *Michèle Coninx* (President of Eurojust) and *Martine Solovieff* (Prosecutor General of Luxembourg), *Frank Cassidy* (Eurojust National Member for Ireland) presented Eurojust's recent work on data retention. He began by introducing the DRD and the reasoning of the CJEU in its *Digital Rights* ruling that declared the invalidity of the DRD *ab initio*. Aware of the impact such decision could have on the fight against serious crime, both nationally and internationally, Eurojust has analysed the legal framework on data retention in Member States. Eurojust concluded that national data retention laws have been struck down in

10 Member States (though in two of these the effect of the decision was temporarily stayed) thus far, while they remain in force in 18 Member States. In five Member States, challenges to the admissibility of evidence have already been lodged. The fragmented legal framework on data retention across the EU undermines the investigation and prosecution of serious crime as well as judicial cooperation in relation thereto.

Working Groups

Participants of the Workshop were divided into four working groups, all of which discussed two topics that reflect practical problems caused by the fragmentation of data retention regimes in Member States (see *below*). The working groups were chaired by *Han Moraal* (Eurojust National Member for the Netherlands), *Francisco Jiménez-Villarejo* (Eurojust National Member for Spain), *Frank Cassidy* and *Lodewijk van Zwieten* (Seconded National Expert for Cybercrime at Eurojust).

TOPIC 1

Current EU framework on data retention: legal and practical impact of the CJEU Judgment in case C-293/12 on national systems and judicial cooperation

In the context of topic 1, participants discussed data retention in relation to: (i) the impact of the CJEU *Digital Rights* judgment in the Member States; (ii) indiscriminate data retention; (iii) access to and use of data; (iv) the role of Eurojust; and (v) possible solutions.

The key conclusions were:

- (i) With regard to the impact of the CJEU *Digital Rights* judgment in the Member States:
- There is a high level of fragmentation in the Member States and the CJEU judgment has magnified the scattered picture of data retention rules across the EU. In some Member States, the judgment has had a major effect, for instance, by invalidating national law on data retention and creating a situation of legal uncertainty or even a legal gap. In other Member States, the CJEU judgment has had, thus far, no or little effect.
 - In some Member States, new legislation on data retention is being prepared to ensure strengthened procedural safeguards in compliance with the Charter of Fundamental Rights of the EU and the CJEU *Digital Rights* judgment.
 - Fragmented rules on data retention across the EU can have an adverse impact on the effectiveness of criminal investigations and prosecutions at national level as well as on judicial cooperation between the Member States. With regard to the latter, specific examples were provided to illustrate that - although the European Judicial Area is based on mutual trust and direct communication between judicial authorities - different retention periods and legal gaps can seriously affect the execution of MLA requests.
- (ii) With regard to indiscriminate data retention:
- Retention of bulk electronic communication for criminal justice purposes must be distinguished from bulk surveillance of data for national security purposes. Judicial and law enforcement authorities carry out criminal investigations in the context of specific serious criminal offences and request metadata for investigation/prosecution purposes on a case-by-case basis. While such investigations may interfere with the rights of

individuals, they are subject to procedural safeguards, such as judicial supervision. Moreover, the evidence can be challenged before the courts and other legal remedies are available.

- Generalised data retention schemes are important, if not essential, for the investigation and prosecution of serious crimes. Data retention must be carried out in a generalised manner as it is impossible to know beforehand whose data will be relevant in the course of a specific criminal investigation and prosecution.
- Generalised data retention is not only a useful tool to link suspects to an offence, but also to delink suspects from an offence.
- There are no equally effective alternatives to data retention. Metadata that are generated by telecommunications (*e.g.* traffic data, location data and other customer-related data) are often the only way to identify a suspect or their whereabouts. These data can also be crucial to decide in a specific case whether it is justified or not to use more intrusive surveillance tools such as telephone interception.

(iii) With regard to access to and use of data:

- Different models on access to data exist in the Member States, depending on, *inter alia*, the nature of the data that is requested (*e.g.* subscriber data, traffic data, location data), or the authority that is required to give the authorisation (*e.g.* an investigating judge, prosecutor, the police and, when provided, an impartial examining judge/court not dealing with the investigation).
- Legal requirements for access to subscriber data tend to be lower than for traffic or location data. In many Member States, the latter require an authorisation, whereas the former do not. In some Member States, however, authorisation by a judge or prosecutor is not required at all (authorisation by the police) or it is, on the contrary, required for all types of data. Moreover, the exact meaning of “judicial authorisation” differs from Member State to Member State.
- Judicial authorisation enables the judicial authority to assess the necessity and proportionality of the requested data. The seriousness of the offence is an important factor that needs to be taken into account during this assessment. Member States use different parameters to define serious crimes, *e.g.* some Member States define serious offences on the basis of the years of imprisonment that are set for a crime while others use a list of crimes. There are also Member States that use a combination of different criteria that specify that all the circumstances and interests (including the strength of the suspicion) of the case need to be assessed. These different approaches in the Member States can lead to different outcomes in the assessment.
- The role of service providers needs to be reconsidered. Service providers from the private sector should collaborate, at all times, with law enforcement and judicial authorities. They should refrain from ‘assessing’ data retention requests on the basis of their own internal policies that can change at any time.
- The processing of MLA requests in relation to data retention tends to be cumbersome and slow. The possibility to address data requests directly to service providers in third States could be explored further. Several participants provided specific examples of where this direct approach to service providers in third States was successful. It was,

however, also specified that much depends on the third State involved and the type of offence. Particularly for terrorism, cooperation tends to be swift.

- Traffic data should be provided by service providers in the Member State where they are offering their services although the data may be stored on servers in other jurisdictions. In this regard, the judgment that the Belgian *Cour de Cassation* delivered in the *Yahoo case!* on 1 December 2015 offers interesting perspectives.
- The Budapest Convention on Cybercrime (2001) can be a relevant legal basis, particularly the provisions on the production order (Article 18(1)(b)) and on trans-border access to stored computer data (Article 32).

(iv) With regard to the role of Eurojust:

- Eurojust can continue to play an important role in assisting judicial authorities in cases where data retention issues rise.
- Eurojust can continue the work carried out thus far in gathering information on national legal frameworks on data retention.
- Eurojust could establish a compendium of existing national legislation and relevant case law to be regularly updated and published on Eurojust's website.
- Eurojust could collect best practice and share this knowledge among practitioners.

(v) With regard to possible solutions:

- The current fragmented legal situation requires intervention at EU level, either via guidelines or via legislation, but always following an impact assessment based on specific difficulties. An evidence-based approach is needed to establish, *inter alia*, the types of data that are needed and the minimum data retention period that is required.
- The development of a standardised, simplified 'smart form' between EU judicial authorities to facilitate data gathering should be explored.
- A clear legal framework will bring legal certainty and be beneficial to all parties involved, *e.g.* suspects, judicial authorities, law enforcement authorities and service providers.
- Any intervention should be TECH NEUTRAL and address procedural guarantees and safeguards in compliance with the Charter of Fundamental Rights of the EU and in line with the CJEU *Digital Rights* judgment.

TOPIC 2

Data retention: admissibility and reliability of evidence after CJEU case C-293/12: national and transnational dimensions

In the context of topic 2, participants discussed data retention in relation to: (i) investigations and prosecutions generally; (ii) evidence; and (iii) judicial cooperation.

The key conclusions were:

(i) With regard to data retention relating to investigations and prosecutions generally:

-
- Data retention is an essential investigative tool. Accordingly, the potential unavailability of this mechanism is undermining investigations and prosecutions. Some Member States have not been affected domestically by the decision of the CJEU in *Digital Rights Ireland Ltd* because their laws remain operative; however, the effect on judicial cooperation is clear.
 - It is not possible to know *a priori* the data that might be necessary in the course of investigations and prosecutions. While it is possible to differentiate technically and legally between categories of data, limiting retention to specific categories or particular persons reduces the effectiveness of investigations and may apply nebulous distinctions, leading to allegations of prejudice, profiling and unlawful discrimination. Moreover, as a matter of law, 'limited' data retention constitutes surveillance or preservation of data (not 'data retention' as such).
 - Addressing one of the shortcomings of the DRD, as described by the CJEU in its ruling, could balance out one or more other shortcomings.
 - Properly regulating access to data is likely to be part of the solution to overcome challenges related to the existing fragmented legal framework in the EU.
 - The fundamental right to privacy can be adequately protected by the introduction of effective procedural safeguards regarding access to data. Such procedural safeguards should include *e.g.* (a) prior authorisation by an independent judicial authority; (b) limitations on the purpose of access and persons entitled to access; (c) management regulations; (d) linkage of access to the seriousness of the crime; (e) assessment of proportionality; (f) evaluation of alternative investigative techniques; (g) destruction of data following the retention period; and (h) exceptions for certain professionals bound by the duty of confidentiality. However, a special regime for certain professional categories may open the way to impunity gaps.
 - Reliable security conditions relating to storage - including location within the EU - are critical.
 - Having a common retention period is crucial: the general view is that it should be longer than six months, preferably a minimum of one year.

(ii) As far as evidence is concerned:

- Communications metadata (which would fall under a data retention scheme) in itself does not yield direct evidence of involvement in a crime. Its evidentiary value lies in the relation with other evidence. Most of the time, the information helps direct the investigation.
- Systems on admissibility of evidence vary significantly throughout the EU. For instance, in some Member States, illegally obtained evidence is, in principle, inadmissible while in others it might be admissible if the offence committed in its gathering is lesser than that under assessment in trial, or there was no intention to consciously violate the privacy right. Likewise, evidence obtained illegally by a third party will be admissible in some countries if law enforcement and judicial authorities were not involved.
- Accessing data retained by telecommunication service providers for billing and commercial purposes assists in balancing the challenges emerging from the abolishment of data retention schemes for the detection, prevention, investigation and prosecution of serious crime. However, the amount and quality of data retained by telecommunication

service providers for commercial purposes may differ among them. Moreover, this avenue is not available in all Member States.

- Requiring telecommunication service providers to maintain a full audit trail will enhance both the reliability and admissibility of evidence.
- The conditions of retention will concern more the authenticity than the admissibility of evidence resulting from data retention schemes.
- The European Investigation Order (EIO) may reduce challenges to the admissibility and reliability of evidence gathered from data retention schemes because of the limited grounds for refusal foreseen.
- An eventual new EU legal instrument could contemplate minimum evidentiary and transparency standards, maintaining a margin of appreciation for the Member States. This could include (a) obligation of retention of data; (b) minimum and maximum data retention periods; (c) harmonisation of conditions of access; (d) common level of accuracy and security of data; (e) maintenance of data within the EU; and (f) irreversible destruction of data at the end of the retention period. With common EU standards, Member States may trust the information provided by telecommunication services providers abroad.
- Minimum procedural/technical standards would be relevant in preserving the chain of custody. However, the decision on admitting evidence in court should remain within the judicial discretion of judges.
- Content data (though subject to higher legal protection) is usually voluntarily submitted to law enforcement agencies by the victim. To carry out investigations and prosecutions effectively it is then necessary to have access to traffic and location data.
- Were the EU to pass a new legal instrument on data retention, national laws remain of essence as they will determine the specific conditions of retention. A reliable system of records and logs of access is crucial.

(iii) In respect of judicial cooperation:

- The differences in data retention regulations – particularly regarding retention periods - are creating significant difficulties in judicial cooperation: the challenges thereby created are best addressed at EU level to put an end to the fragmentation of data retention legal frameworks across the EU.
- The status of evidence gathered abroad varies considerably, from no regulation of the matter to the presumption of admissibility and the application of standards applicable in the forum State. Evidence illegally obtained abroad might be admissible in certain jurisdictions unless it was shared for purposes other than its use in court. For others, the presumption of admissibility will be rebutted when it would otherwise make the process unfair; a serious breach of the right to privacy could ground a decision of the judge on the (in)admissibility of the evidence.
- In some Member States where data retention laws are no longer operative, it is unclear whether it would be possible to use evidence in court that resulted from data retention schemes voluntarily provided by another State. In others, such evidence would be ruled admissible if it had not been gathered at the request of the forum State, even though the latter could not internally collect and use it as evidence.

- Several examples were advanced by participants whereby differences in domestic legislation on data retention hampered investigations and prosecutions in other Member States and third States. The recent terrorist attacks in Paris provide a powerful example of how investigations are affected by the lack of data retention schemes in some of the affected countries.
- Examples of cases where data retention proved crucial to successful investigations, prosecutions, and or defence would assist the Commission in an impact assessment for potential new legislation. Eurojust, with the assistance of national authorities, may be well placed to collate such case illustrations.

Meeting of the Consultative Forum (11 December)

The 10th meeting of the Consultative Forum was convened and chaired by *Martine Solovieff*. The meeting was opened by *Michèle Coninx*. *Maija Andrijauska* (Prosecutor of the International Cooperation Division of the Prosecutor General's Office of Latvia) provided a brief overview of the activities of the Forum under the Latvian Presidency (January to June 2015).

Session I – The CJEU’s Annulment of the Data Retention Directive: Practical Implications for Investigations and Prosecutions

Session I was devoted to the effect the current fragmented legal framework in the EU on data retention may have on the fight against serious crime and judicial cooperation in relation thereto, as analysed during the Workshop of 10 December.

Frank Cassidy and *Francisco Jiménez-Villarejo* reported the outcomes of the working groups of the preceding day (see *above* Topic 1 and Topic 2).

Session I proceeded with the speeches of the distinguished guest speakers.

François Biltgen (Judge at the CJEU) explained the reasoning of the CJEU in *Digital Rights Ireland Ltd*. He highlighted that mass retention of data as provided for in the DRD constitutes a breach of the right to privacy (Article 7 Charter of Fundamental Rights of the EU (CFR)). Access to such information by law enforcement agencies amounts to additional interference with the right to privacy and entails a breach of the right of protection of personal data (Article 8 CFR). Such interference was not justified under Article 52(1) CFR since the limits imposed by the principle of proportionality (especially the requirement of strict necessity) were not complied with. To illustrate this, (i) the duty of confidentiality by certain professionals was not taken into account; (ii) no link was established between the retention of data and a risk to public security; (iii) the obligation of retention was not limited in time or geographically; (iv) no distinction was made between different categories of data; and (v) the retention of data targeted unsuspecting persons. Mr Biltgen concluded that despite the invalidation of the DRD, national laws must comply with the terms of the e-Privacy Directive.¹ Data protection authorities and domestic jurisdictions must apply and respect the CFR as interpreted by the CJEU. Furthermore, in the absence of applicable legislation within the realm of EU law, Member States must nonetheless comply with the European Court of Human Rights (ECtHR).

¹Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Dean Spielmann (former President of the ECtHR) expounded on the 'évolutive' interpretation of the ECHR which permits continuously taking into account and responding to the challenges and demands resulting from new technologies. While the retaining and processing of personal data may be essential for protecting society against terrorism and other dangers, this may not justify all measures and intrusions into the fundamental rights of individuals. Mr Spielmann called upon the relevant case law of the ECtHR that contributed to the effort of striking a balance - in the realm of investigations and prosecutions - between the right to privacy and the need to protect citizens, with regard to measures such as wiretapping and secret surveillance. Likewise, attention was drawn to access to personal data as processed in public archives, judicial files, and databases of intelligence services. In its balancing assessment, the ECtHR takes into account the (i) circumstances in which public powers may resort to, and terminate, certain intrusive measures; (ii) length of the measure; (iii) conditions for the access to, use, storage and destruction of personal data; (iv) existence and conditions for the exercise of the right of access to court and to an effective remedy; and (v) notification of the data subject and access thereby to information necessary to exercise the rights of access to court and to an effective remedy.

The speeches of both guest speakers were followed by a general discussion in which several Forum members spoke. The outcome of the discussion and the written contributions submitted in advance by Forum members² can be summarised as follows:

Conclusions of the Consultative Forum on Data Retention

1. Data retention is a fundamental investigative tool. The prevention, detection, investigation and prosecution of serious offences in several Member States have been affected by the annulment of the DRD. Most Forum Members that consider otherwise, base their position on the fact that national laws have not been challenged or remain operative.
2. Where national data retention laws have been struck down, access by law enforcement agencies to retained data is limited or non-existent given that there is no longer an obligation for telecommunication service providers to retain data or because this obligation covers only certain categories of data.
3. Challenges to the admissibility of evidence have been lodged in some Member States.
4. Forum members note that judicial cooperation also faces significant challenges. Cooperation is affected both within and outside the EU, whereby some countries are in the position to share more data than EU countries. Likewise, different retention periods seriously affect the execution of MLA requests.
5. The fragmented legal framework may cause further difficulties in parallel investigations, resolution of conflicts of jurisdiction (as the choice of best forum to prosecute may be undermined), the efficiency of JITs as well as in respect of the obtainability and admissibility of evidence. Judicial cooperation has been affected particularly with Member States where data retention legislation has been invalidated.

² Written contributions were received from 18 Forum members from the following Member States: Austria, Belgium, Cyprus, Estonia, Finland, Germany, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Spain and the United Kingdom.

6. Judicial cooperation could be enhanced by expanding the possibilities to access data stored abroad under the 2001 Council of Europe Convention on Cybercrime (the so-called 'Budapest Convention'), with negotiations to that effect being led by the EU rather than Member States.
7. The Consultative Forum looks forward to further guidance and assistance from the ruling of the CJEU in case C-203/15 (*Tele 2 Sverige*). This case (and a subsequent preliminary reference from the UK Courts in case C-698/15) seek to clarify the effect of the judgment in DRD case C-293/12 and will be pertinent to any future EU work on the issue.
8. Considering the different regimes across the EU and the subsequent significant difficulties encountered in judicial cooperation, the Consultative Forum calls for an EU solution on data retention. A European common framework to harmonise retention of, and access to, data is deemed necessary. The Consultative Forum therefore invites the European Commission to take action in this regard (possibly after an impact assessment) in line with the requirements established by the CJEU in *Digital Rights Ireland Ltd (C-293/12)*. Notably, the Forum recommends:
 - Establishment of an obligation of retention of data under EU law.
 - Consideration should be given to the appropriate conditions that should apply in relation to access to retained data, *e.g.*: (i) be limited to serious forms of crime (for instance, the crimes listed in Article 83 TFEU and/or a threshold of minimum penalties attached to the crime could serve as guidance); (ii) comply with the tests of proportionality and strict necessity; and (iii) attempt to balance confidentiality duties binding certain professionals.
 - Consideration should be given to the appropriate security and storage conditions to be applied to retained data.
 - Common minimum and maximum data retention periods should be foreseen as well as the obligation to destroy data afterwards.
 - Additional procedural safeguards may include (i) notification of the person concerned after a period of time, and (ii) right of the data subject to require the deletion of data under certain terms.
9. At national level, different rules could apply according to the type of data in question (traffic data vs location data). Regarding control over access to retained data, it is important to ensure expedited access thereto in urgent situations because of direct threats to public order and security; in such situations, consent *ex post* might be a solution.
10. The Consultative Forum invites Eurojust to continue its analysis of the impact of the annulment of the DRD on national systems and, through an evidence-based approach, collect practical examples together with our prosecution services. This will be of great support in the context of the process leading to a possible new EU instrument on data retention.
11. The assistance of Eurojust would also be welcome in analysing potential problems in

judicial cooperation, highlighting good practices and guidelines in relation thereto, and continuing the analysis of national legislation on data retention.

12. Eurojust could engage further in close cooperation with Europol's EC3 and equivalent expert networks so as to transmit relevant information to the Member States. Good cooperative relationships with States where the registered offices of the largest private service providers are located, *e.g.* the United States, are also important, and the fact that there is a US Liaison Prosecutor at Eurojust can offer interesting perspectives for fruitful cooperation.
13. The recent terrorist attacks in France have alerted all to the challenging times the world is experiencing, whereby a high level of security for all citizens cannot be guaranteed without some level of intrusion of the right to privacy. This notwithstanding, it is crucial to strike the right balance between the right to privacy and the security of the overall community.

Session II – Terrorism: Towards a Common Judicial Response to Foreign Terrorist Fighters

During Session II, the Forum was updated on Eurojust's work in combating the foreign terrorist fighter phenomenon and discussed the criminal justice response.

Ms Coninx opened the session by presenting a summary of the third Eurojust report, *Foreign Terrorist Fighters: Eurojust's Views on the Phenomenon and the Criminal Justice Response*, with particular emphasis on some of the new challenges identified by Eurojust in investigating and prosecuting foreign terrorist fighters. As with previous editions, the report is based on Eurojust's cases that deal with foreign terrorist fighters, information provided to Eurojust by national correspondents on terrorism and other national practitioners, as well as on the experience Eurojust has gained in this field over the past three years. Even though there has been an increase in the number of cases referred to Eurojust, *Ms Coninx* stressed that there are still quite a number of challenges faced by practitioners when investigating and prosecuting terrorism cases. These include: i) fragmentation of national legal frameworks, which might jeopardise judicial cooperation; ii) difficulties related to gathering, sharing and securing admissibility of electronic evidence; and iii) insufficient exchange of information among competent authorities. In this context, *Ms Coninx* referred to the need to promote better use of the Eurojust National Coordination System and the National Correspondents for Terrorism, and to step up judicial cooperation, particularly with key third States. She also mentioned the need to consider developing the European Criminal Records Information System and to consider the opportunity of extending it to third country nationals. One of the novelties of the 2015 Report presented during the meeting relates to the efforts currently being made by Member States in identifying innovative judicial responses to this phenomenon, including various measures to develop de-radicalisation and disengagement programmes.

The main conclusions stemming from the discussion are:

Conclusions of the Consultative Forum on Terrorism

1. The Consultative Forum condemns the Paris attacks of November 2015 and recognises the increased terrorist threat and global challenge posed by the phenomenon of foreign terrorist fighters.
2. Forum Members listened attentively to the lessons learned during the tragic recent attacks. These include the importance of the early involvement of the judiciary, the speedy exchange of information with other Member States, and the positive feedback on the use of JITs in such situations.
3. The Forum supports the ongoing extensive efforts of Eurojust to assist Member States that are reflected in the steady increase of cases referred to Eurojust for coordination and assistance.
4. The Forum welcomes the findings of the third Eurojust Foreign Fighter Report, and notes its main conclusions and recommendations, particularly the need to consider input from the judiciary in de-radicalisation and disengagement programmes and to making greater use of the ENCS and of the National Correspondents for Terrorism.
5. The Forum calls for a common European and multidisciplinary approach as well as the fostering of judicial cooperation with key third States, also with the support of Eurojust.
6. Furthermore, the Forum calls upon the EU to assist judicial practitioners in overcoming major challenges which persist, such as the gathering and admissibility of e-evidence, the transmission and judicial use of information from the intelligence services and the need to take a European approach to dismantle organised criminal groups behind the trafficking of weapons.

Session III – Illegal Immigrant Smuggling: Challenges and Best Practices in Investigations and Prosecutions

Session III was devoted to the exchange of views among Forum members in identifying challenges in the investigation and prosecution of illegal immigrant smuggling cases and possible solutions thereto, with a view to supporting national practitioners and increasing judicial cooperation.

Ms Coninx briefly presented the background paper, with particular emphasis on the many actions taken by Eurojust since the meetings of December 2014 and June 2015, when Forum members had the opportunity to discuss different aspects related to the current migration crisis from a judicial perspective. In particular, the Forum was informed of the setting up of the Eurojust Thematic Group on Illegal Immigrant Smuggling in September 2015, in line with one of the conclusions from the Forum meeting of December 2014, and the organisation of the upcoming tactical meeting on illegal immigrant smuggling.

Cyril Lacombe (Assistant to the National Member of France and Eurojust Contact Point for Smuggling of Migrants) gave an overview of written responses received from Forum members to a set of questions circulated prior to the meeting. In particular, Forum members were asked

about the main challenges faced by practitioners when prosecuting illegal immigrant smuggling cases and the value of Eurojust's assistance in their daily work.

Following this presentation, the Chair opened the session to a general discussion.

The representative of Europol took the floor during the open debate to give a short presentation of Europol's main initiatives in this field. Reference was made, *inter alia*, to the (i) Joint Operational Team Mare, a specialised team of experts focusing on human smuggling across the Mediterranean and Aegean seas and the subsequent secondary movement to destination countries; (ii) EU Internet Referral Unit, which tackles the use of social media by smugglers; and (iii) Europol Migrant Smuggling Centre established in 2015. The intense and fruitful cooperation with Eurojust was also mentioned, not only in strategic initiatives, but also in some significant operational cases. Stepping up the fight against illegal immigrant smuggling requires the prompt exchange of information at an early stage of investigation (between Member States and between Member States and Europol) as well as close cooperation among police, prosecutors and the judiciary.

The representative of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex) also took the floor during the open debate to describe the support Frontex can provide to Member States faced with urgent and exceptional migratory pressure at its external borders. In particular, reference was made to Operation Triton in the Central Mediterranean, Operation Poseidon in the Aegean Sea, as well as the two EU Regional Task Forces in Italy and Greece.

The representative of the Fundamental Rights Agency (FRA) updated the Forum on FRA's past and ongoing work in the field of illegal immigrant smuggling, including the study on the *Criminalisation of migrants in an irregular situation and of persons engaging with them*.

The main conclusions stemming from the discussion and the written contributions received from Forum members³ can be summarised as follows:

Conclusions of the Consultative Forum on Illegal Immigrant Smuggling

1. The Forum considers that cooperation among Member States and with key third States, particularly for the exchange of information and execution of MLA requests, is crucial in illegal immigrant smuggling cases. However, practitioners continue to experience difficulties in this field.
2. Forum members consider that the collection of evidence is complex, also given that many evidentiary measures require execution in the country of origin. This undermines the identification of criminals among migrants. The current terms of the Dublin II System create additional difficulties. Furthermore, there are challenges related to gathering the testimony of victims, as they are often coached or refuse to cooperate, and in checking the identity of migrants as they often travel with forged or no documents at all. Therefore, the Forum believes that better systems for identifying

³ Written contributions were received from 20 Forum members from the following Member States: Austria, Belgium, Bulgaria, Cyprus, Estonia, Greece, Finland, Germany, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Spain and the United Kingdom.

migrants and gathering their testimonies are necessary.

3. A further difficulty relates to the lack of reliable translators, considering the amount of documents that require official translation in proceedings and the less common languages often encountered.
4. Considering the complexity of illegal immigrant smuggling cases, Forum members consider parallel financial investigations of pivotal importance, as well as the monitoring of social platforms. Some Forum members suggest that consideration should be given to supporting investigations by special investigative techniques (*e.g.* surveillance).
5. The Forum is well aware of the specific challenges posed by smuggling illegal immigrants by the sea (particularly the assertion of jurisdiction and the execution of operational actions on the high seas). Several Forum members suggest the Consultative Forum should act as a 'strong awakening voice of the European institutions' regarding illegal immigrant smuggling by sea, highlighting the difficulties faced by frontline Member States.
6. Forum members highly value the support and assistance provided by Eurojust. In this context, the following points were mentioned:
 - a. The creation of the Thematic Group, which the Forum believes will greatly assist prosecutors in identifying and analysing obstacles and best practice stemming from national cases and in analysing gaps in legislation, also with a view to making proposals to the Commission;
 - b. The organisation in early 2016 of the first tactical meeting on illegal immigrant smuggling;
 - c. The support provided to practitioners through Eurojust's operational tools, including coordination meetings, coordination centres and JITs.
7. Furthermore, the Forum suggests Eurojust continues promoting cooperation with key third States, also through the establishment of new contact points in countries of origin, ensuring close cooperation with judicial contact points in the hotspots, and making greater use of Articles 6 and 7 of the Eurojust Decision.
8. The Forum also welcomes all efforts of other EU agencies, including Europol, Frontex and FRA, to counter the migration crisis and encourages and praises the close cooperation between them.
9. Considering the inner cross-border nature of illegal immigrant smuggling, the Forum calls for a common EU approach to this phenomenon, which should at least include some degree of harmonisation of the crime and applicable sanctions. The ongoing work on the revision of the so-called '*Facilitators Package*' under the auspices of the European Commission was praised, though the lengthy procedure emphasises the need for more expedited responses.
10. The Forum considers with interest the French suggestion to create an 'operational group' to enhance regional cooperation among some key transit and destination countries in the North of Europe (including France, the Netherlands, Belgium and the

United Kingdom).

11. Finally, the Forum agrees to support, possibly via Eurojust, the European Commission in its call for the gathering of additional information on the implementation of relevant EU legislation.

Session IV – Future Perspectives: Working Methodology of the Consultative Forum

To prepare for this Session, a questionnaire was circulated to Forum members at the initiative of the Luxembourg Presidency, in coordination with the Board of the Consultative Forum. The questions addressed the content, format and frequency of Consultative Forum meetings, as well as the practice of combining Eurojust strategic seminars with Consultative Forum meetings. Replies were received from all Forum members. During the discussion, Forum members considered the results of the questionnaire which were presented by *Olivier Lenert* (Eurojust National Member for Luxembourg). In particular, Forum members were advised that most replies were in favour of having just one meeting of the Consultative Forum per year, preferably under joint EU Presidencies, either at the end of June or beginning of July. With regard to the choice between combining Consultative Forum meetings and Eurojust strategic seminars, or separating them, no clear preference was expressed. Finally, most replies confirmed that the topics discussed in Consultative Forum meetings have thus far met Forum members' expectations. Several respondents also proposed topics for future meetings. In this context, one Forum member highlighted the importance of consulting with Prosecutors General on the agendas prepared for Consultative Forum meetings so that such agendas can be tailored. The importance of Prosecutors General and Directors of Public Prosecutions attending Forum meetings and the distinction between participants of Forum meetings and strategic seminars, that deal with issues of a technical nature, was also stressed.

The main conclusions stemming from the discussion are:

Conclusions of the Consultative Forum on Working Methodology of the Forum

1. By a large majority, Forum Members are in favour of having just one meeting of the Consultative Forum per year, preferably under joint EU Presidencies, either at the end of June or beginning of July.
2. Forum members take note that no clear preference has been expressed with regard to the choice of combining Consultative Forum meetings and Eurojust strategic seminars or separating them. Future Presidencies will discuss the matter directly with Eurojust, taking into account Eurojust's planning and budgetary constraints.
3. Most Forum members are satisfied with the topics discussed thus far in Consultative Forum meetings. In their written replies, Forum members made a number of proposals for future topics and working methods. Such proposals could be examined in preparation for future meetings.

Closing Session

Open debate by Forum members

Andrzej Seremet (Prosecutor General of Poland) bade farewell to the other Forum members by announcing that he was leaving office soon. The Chair and Ms Coninx paid a special tribute to Mr Seremet for his valuable contribution and continuous support to the work of both the Consultative Forum and Eurojust.

Next Meetings of the Consultative Forum

Albert van der Kerk (Chief Public Prosecutor for international affairs, Public Prosecution Service of the Netherlands) and *Jozef Szabó* (Deputy Prosecutor General, Prosecutor General's Office of the Slovak Republic) announced their decision to organise a joint meeting of the Consultative Forum, thus applying the new approach starting from their own Presidencies. This first joint meeting of the Consultative Forum will be convened on 3 June 2016, with the support of Eurojust and, possibly, in combination with a Eurojust seminar to be held on 2 June. Currently proposed topics were the following: strengthening judicial cooperation against cybercrime, incl. evaluation of investigating practices in joint operations and use of existing legal instruments; setting up of a network of specialised prosecutors against cybercrime; multidisciplinary approach to fighting organised crime; and recovery of criminal assets. At the same time, both Presidencies confirmed their intention to keep a flexible approach, so that the agenda of the Consultative Forum can consider major priorities, such as illegal immigrant smuggling and terrorism, and any other possible new policy or legislative developments of relevance to Forum members.

Meeting Conclusions

The main conclusions reached during the meeting were presented and provisionally circulated to all Forum Members after the meeting. As usual, the report of the meeting, including more detailed conclusions, will be circulated to all participants and transmitted to the relevant EU institutions.