Council of the European Union

Brussels, 6 June 2016
(OR. en)

9368/1/16
REV 1

LIMITE

JAI 478
COSI 92
FRONT 224
ASIM 80
DAPIX 80
ENFOPOL 157
SIRIS 90
DATAPROTECT 57
VISA 165
FAUXDOC 23
COPEN 172

NOTE

From:	Presidency
To:	Council
No. prev. doc.:	8437/2/16 REV 2
Subject:	Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area

The recent terrorist attacks in Paris and Brussels, continuous terrorist incidents outside the EU and the ongoing migration crisis have shown the importance of investing in swift, effective and qualitative information management, information exchange and accompanying follow-up of information to tackle migratory, terrorist and crime-related challenges. This was recently confirmed by the Council on 20 November 2015, by the European Council on 17 and 18 December 2015, by the Justice and Home Affairs Ministers and representatives of EU Institutions in their statement on 24 March as well as by the Council on 21 April 2016.

The security and migratory challenges are complex and interconnected. Efforts to tackle them are already undertaken between the various JHA domains – for example, an effective border-management as an integrated part of the EU's security architecture to address illegal immigration, terrorism and crime.

The Presidency has taken the ambitious initiative to set up a Roadmap with necessary actions to improve information management and the cross-border exchange of information, including interoperability of systems. The purpose is to support operational investigations, especially in counter-terrorism - realising there is a close connection between terrorism and crime - and to swiftly provide front-line practitioners such as police officers, border guards, public prosecutors, immigration officers and others with comprehensive, topical and high-quality information to cooperate and act effectively.

The Presidency started discussing the counter-terrorism related actions during the informal JHA Council on 25 January 2016 and also discussed the issue during the JHA Council on 21 April with a debate also focusing on the Commission Communication Stronger and Smarter Information Systems for Borders and Security. Based upon the outcomes and the new developments within the EU, the result of this combined effort is laid down in the annex to this Presidency note.

This Presidency document contains **a Roadmap with specific, practical short- and medium-term actions and long-term orientations to enhance information management and information exchange in the Justice and Home Affairs (JHA) area.** It builds on the ongoing good work over the past years[1], and is meant to be **a living document.**

[1] E.g. the Council conclusions in 2013 and follow-up activities of the European Commission Communication on the European Information Exchange Model (EIXM).

It takes into account the outcome of recent discussions in the Council (the Justice and Home Affairs Council on 21 April[2], the joint COSI/SCIFA on 17 April, COSI on 3 and 4 March[3] and DAPIX on 26 January and 15 March 2016[4]) as well as the recently updated Information Management Strategy (IMS)[5] and the recent Commission *Communication Stronger and Smarter Information Systems for Borders and Security* of 6 April 2016[6].

Developing the Roadmap, putting it into practice and monitoring the results and reviewing and updating it requires **a common approach from the Council, the Commission, the EU Counter-Terrorism Coordinator (CTC) and EU Justice and Home Affairs agencies. It aims to support operational investigations and practitioners - working on the street, at border crossing points, conducting investigations, assisting migrants, and assessing visa applications - in effectively and efficiently performing their day-to-day work.**

This Roadmap, being a living document, provides a **coherent framework for a more integrated EU information architecture[7] in the JHA area,** and includes an analysis of key JHA broad challenges, principles and horizontal guidelines and a way forward to monitor and follow-up on the actions in the Roadmap **(Chapter 1).** It also includes dedicated information exchange and information management actions in the following domains taking into account the differences in legal framework of those areas:

– **law enforcement including judicial cooperation in criminal matters (Chapter 2),**

– **detection of persons involved in terrorism and their travel movements (Chapter 3),**

– **border management and migration (Chapter 4);**

---

2 7711/16 JAI 264 COSI 54, 7726/16 JAI 266 COSI 55

3 DS1129/16

4 5180/16 JAI 20 DAPIX 5

5 The Council conclusions in 2014 and follow-up activities updating the EU Information Management Strategy for Internal Security

6 7665/16 JAI 258 ASIM 50 RELEX 239

7 Acquiring an integrated information architecture is an ever evolving process which requires a joint-up effort and time, bearing in mind differences between Member States, policy areas, legal conditions, technical and financial requirements and the human factor.

Although these three chapters (Chapters 2, 3 and 4) focus on different areas, it is important to highlight the interlinkages between them in this Roadmap. This will contribute to ensuring the cooperation between the authorities and agencies active in the three policy areas and the interoperability between information systems.

The Presidency offers the following strategic considerations for further political discussion and political guidance, fully aware of the fact that the Ministers for Justice and the Interior (JHA) on 24 March 2016 decided to further step up implementation of measures already decided upon:

- First and foremost the Presidency is seeking a political commitment to feed and use the information systems to the maximum extent, as a *conditio sine qua non* for achieving an efficient sharing of information. A political commitment to feed and use the existing data systems and act accordingly will enhance trust between operational actors (variations in the JHA challenges Member States face may influence the amount of information shared)**.** The Presidency seeks a political commitment to share all relevant information unless there are legal or operational reasons not to do so. When assessing if such reasons are applicable the operational interests of other Member States and where applicable EU agencies in acquiring information are fully taken into account. Regular updates on the actual feeding and use of existing data systems by the EU CTC with input from the Commission and relevant agencies are necessary, in order to identify lessons learned and support continuous improvement. In this context it goes without saying that the capability of Member States to collect information, especially to follow up on leads about possible terrorists, and to assess the terrorist threat in general, is of great importance.

- Privacy and data protection are core values, fundamental rights and norms in the EU. Member States have the obligation to protect and ensure the security of its citizens. Therefore the protection of citizens and the principles of privacy and data protection are complementary and mutually reinforcing. In striking the right balance new methods to safeguard information and enabling various degrees of access rights in one system should be taken fully into account. This shall be preceded by a thorough analysis of information needs considering law-enforcement, counter-terrorism, migration and border management processes. These conditions shall be taken into account by the Commission when developing the new legal proposals for SIS, VIS and Eurodac, in particular as regards access to these systems for law enforcement and counter terrorism purposes.

- In the context of interoperability, a complex issue, a single-search interface is of great importance. As a matter of priority it should be implemented through one-stop-shop information solutions at national and European level which provide single interfaces for Member States for feeding and searching national and international information systems. A single search interface provides important progress for border guards, police, immigration and custom officers conducting checks and for operational investigations, taking into account the need of information of the specific organisation. The Commission Communication on Stronger and Smarter Information Systems for Borders and Security mentions three other dimensions of interoperability (i.e. the interconnectivity of information systems, the establishment of a shared biometric matching system in support of various information systems and a common repository of data for different information systems), which also need to be analysed in the medium and longer term. Proposals on the legal, technical, operational and financial consequences of all four dimensions, as well as on prioritisation of interoperability initiatives should be studied and developed by the High Level Expert Group of the Commission on Information Systems and Interoperability. The progress and the results are to be discussed in COSI and where appropriate in other Council bodies.

- Possible short term and long term solutions should be found to bridge the gap between Schengen, non-Schengen Member States, and Member States who are partially using the Schengen acquis pending a permanent solution to this issue-in terms of provision and access to EU information databases. This should be taken into account by the Commission in the new legal proposal for SIS and VIS. Technical solutions to bridge the gap until that time need to be sought as well.

- There is a clear need for progress towards proactive and systematic sharing of criminal records data for people convicted of offences relating to terrorism and serious and organised crime, in particular with the appropriate authorities at the border. Consideration should be given to what practical steps could be taken to achieve this, including which systems (other than the ECRIS system) would offer the most effective means of doing so.

As tangible actions are necessary to ensure that information is shared efficiently and in real-time, the Presidency invites the Council to:

- ***endorse*** *the policy framework hereafter, especially the principles of information exchange, and* ***endorse*** *the actions (ongoing and new) and timelines thereafter****, taking into account that this is a living document that can be adjusted to future developments and insights.*** *Progress is to be strategically monitored by COSI in coordination with other relevant preparatory bodies of the Council, the Commission and the EU Counter Terrorism Coordinator (CTC), on the basis of progress reports prepared by COSI in cooperation with the CTC, the Presidency and the Commission. The Council will be regularly informed on progress made and in any case when political decisions are necessary; and*

- *agree to ensure that EU and international databases are properly filled and used by national authorities responsible for counter-terrorism, law enforcement, migration and border management. The quality of information being shared is of equal importance as the quantity. Monitoring will be done by COSI, taking into account the Schengen evaluations, in close cooperation with the Commission and the EU CTC. COSI will report to the JHA Council.*

CHAPTER 1: FRAMEWORK FOR A MORE INTEGRATED EU INFORMATION ARCHITECTURE

1. Challenges

Front-line officers are addressing a range of challenges and they need access to information to take effective action. They often need similar or even the same information, which may include detailed information on persons, the goods they are carrying or transporting, financial means and more in-depth information on the background of persons and possible networks. In order to effectively carry out their duties, officers must apply all agreed safeguards, in particular on fundamental rights, collect, check and connect the right information at the right time in the right place to undertake effective action.[8]

For those purposes, legal, policy, operational and technical instruments have been put at their disposal at national, EU and international level. However, there are different (national and European) legal, technical and operational challenges in the interoperability of systems, different user groups and the different retention periods of personal and biometric data in these systems. Moreover, the risks of vital information gaps among (categories of) practitioners is ever present, for example due to

a) limited availability of information (e.g. on specific types of terrorist travellers);

b) limited access to information or a limited timeframe for identity and security checks on persons at borders (e.g. due to a complex legal base or technical obstacles);

c) Member States and their authorities not being connected to systems;

d) a suboptimal sharing of information based on an overly strict application of the need-to-know principle affecting in particular ongoing investigations and the possibility to undertake immediate action.

[8] Inspired by the Council conclusions on the EU Information Management Strategy

Underpinning elements of this situation are:

1. The **human factor**: information will be effectively exchanged only if there is trust among the practitioners at national and international level (including trust between the different organisational / institutional structures). Also, the complexity of available tools and procedures, different law enforcement traditions, as well as varying expertise among practitioners, may cause errors.

2. **(Constitutional) legal requirements**, such as criminal procedural law, data protection requirements, purpose limitations etc. Information systems and information exchange procedures have been developed in various institutional, legal and policy contexts. These conditions are binding, in substance important and well substantiated by the legislative process on the basis of commonly determined needs. However, they have an effect on what is and should be feasible regarding the exchange of information and the follow-up actions to be taken, for example due to the different set-up of databases, divergent access to data of relevant authorities and lack of hit/no hit possibilities.

3. **Limited resources** (personnel, financial means and time) at national and European level. Consequently practitioners and their authorities may struggle to address all the challenges they face.

4. **Technical/system requirements** for swift and effective information management and information exchange actions do not exist to the extent necessary, especially in the area of inter-institutional information exchange and there are shortcomings in the functionalities of existing information systems. The latter problem is partially due to the fact that existing systems in use (e.g. SIS II, VIS, EURODAC, ECRIS other) were not created based on a systematic approach and complete process analyses of the work of the intended users, but as a solution for particular problems in specific areas.

5. **Existing legislation[9], policies[10] and procedures[11] on EU information management and exchange in the JHA area have not been implemented fully** and the capabilities of JHA agencies have not been used to their full extent to support Member States.

2. Principles

A coherent interconnected approach to improve information management, information exchange and intelligence-led follow-up actions should be pursued in accordance with the following principles:

A. Full respect of fundamental rights and data protection rules

Requirements are: continuously assessing the necessity of a measure, applying requirements of subsidiarity and proportionality and carrying out an accurate risk management. It will also require embedding personal data protection in the technological basis of a proposed instrument (privacy by design), limiting data processing to what is necessary for a specified purpose while not missing information that is operationally relevant, and operationally and legally substantiating the need for (a degree of) access to information for (a category of) practitioners.

---

9 E.g. the Prüm decisions, the Swedish Framework decision

10 E.g. Council conclusions following the Commission Communication on the European Information Exchange Model (EIXM) of 6 and 7 June 2013 (9811/13), Council Conclusions on an updated Information Management Strategy (IMS) for EU Internal Security of 5 December 2014 (15701.1.14 REV 1), Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism, 20 November 2015.

11 The Manual on Law Enforcement Information Exchange, the SIRENE Manual

B. An information-centred approach based on process analysis

A prerequisite is: the continuous pursuit of the principle of availability including accompanying conditions[12], the principle of equivalent access and quality of information at national, European and international level. Requirements are: availability of information to all relevant competent authorities with due attention to data protection concerns; and in order to support strategic use of information to prevent threats, (risk) analysis, decision making and to prioritise actions, more focus on data quality including clarity on what type of (topical) information to share for what purpose respecting clear criteria and enabling effective follow-up actions; focus on the other elements outlined in the recently updated Information Management Strategy (IMS) for EU Internal Security.[13]

C. A practitioner centred approach building upon trust and operational needs

Requirements are: a continuous investment in mutual trust at all levels; bottom-up design with a pro-active focus on user-friendliness of information processes and accompanying instruments in which day-to-day practices on the ground are the starting point for authorities involved in the development of solutions; emphasis on training in effectively fulfilling roles in (international) information processes; a reflection on the effectiveness of existing practices and the root causes of deficiencies should be continuous; an exchange of good practices between the Member States on user-friendliness of information systems and processes through training, meetings, catalogues and online should take place.

---

12 These accompanying conditions are a) the exchange may only take place in order to perform proportionate and necessary legal tasks; b) the integrity of the data to be exchanged must be guaranteed; c) the need to protect sources of information and to secure the confidentiality of the data at all stages of the exchange; d) supervision of respect for data protection, and appropriate control prior to and after the exchange must be ensured; e) individuals must be protected from abuse of data and have the right to seek correction of incorrect data.

13 15701/1/14

D. Full implementation and use of existing information management and information exchange instruments and taking informed decisions on new initiatives

A prerequisite is: sufficient experiences with the full potential of existing instruments and assessing their effectiveness; coherence in implementation and application of instruments. Requirements are: continuous monitoring at the level of the Commission (e.g. Schengen evaluation and Monitoring mechanism), and the Council. These efforts should act as a basis to inform authorities when developing new initiatives addressing evolving operational needs.

E. Effectively ensuring interconnectivity of European initiatives with national processes

A prerequisite is: the existence of coherent integrated national information architectures. Requirements are: pursuing standardisation of requirements, such as on quality, supply and searching of data, and enabling (national) tailor-made solutions to integrate international systems in a national information environment, while bilateral and international information exchange processes are taken into account when developing those solutions; Member States themselves are primarily responsible for guaranteeing coherence in all these processes, responsiveness to operational needs and for enabling required tailor-made solutions.

F. Pursue the systematic sharing of information with other Member States and EU agencies and bodies

Prerequisites are: systematic sharing of information to enable real time analysis taking into account the required capacity and cross-border operational actions to avoid information gaps and duplication of activities; efficient information exchange between EU agencies (in particular Europol, Eurojust and Frontex) where their mandates and legal provisions provide such possibilities. Requirements are: fully taking into account the respective mandates, valid operational and legal reasons (exemptions[14]) for not sharing information, continuously being critical on the application of such exemptions, considering rapidly evolving circumstances and limited windows of opportunity for the timely sharing of relevant information.

[14] Article 4 TEU and Articles 72 and 73 TFEU and source protection, protecting an ongoing investigation, avoiding a life threatening situation, no authorisation to share information provided by a third party.

G. Information management and information exchange remains a means to an end[15]

Requirements are: priorities set for information management and exchange must correspond to operational needs and priorities; the most operational- and cost-effective solutions with a clear allocation of responsibilities should be pursued including at national level, with effective support and monitoring of international information exchange and the lowest possible administrative burdens.[16]

3. Horizontal Guidelines

Apart from the above-mentioned principles and the actions set out in the dedicated chapters, the following horizontal guidelines should be brought forward, with priority to the first two matters.

- **Pursue interoperability solutions, including but not necessarily ending with implementation of a single search interface following the development of (a) technical solution(s).** As a prerequisite, such efforts should fully take into account and enable data protection requirements, mutual legal assistance provisions and the full application of the information owner principle. The solutions can provide efficiency gains in providing and searching/requesting information but should ensure that relevant EU agencies can fulfil their mandate and support Member States.[17] Single search solutions should be brought forward by building on already existing good practices available at national and international level. For the implementation action 4 in Chapter 2 is applicable.

---

15 16637/09 + COR 1

16 In the area of police cooperation Single Point of Contact – SPOC - in each Member State as a 'one-stop shop' for international police cooperation, operating 24/7

17 Examples of technologies can be found in relation to FIU.net (using the Ma3tch technology) or the ADEP project within the framework of the current IMS action list

- **Explore the added value and the requirements of a shared biometric matching service for all relevant information systems.**[18] The interoperability of biometric identifiers enables the use of a shared biometric matching service for several information systems and will enhance the ability of authorities to verify accurately the identity of a person. The service shall respect personal data protection rules. The High Level Expert Group on information systems and interoperability, which the Commission will set up, is invited to explore the question and to inform the Council of its findings.

- **Following an explicit request from the Council explore, the legal, technical, operational and financial implications of:**

  a) interconnectivity solutions whereby systems can consult one other, where appropriate and subject to the principle of the data owner retaining control of the data they provide;

  b) common repository of data (architectural solutions at a decentralised and/or centralised to be determined). The repository would allow for the recognition of connections and provide an overall picture by combining individual data elements stored in different decentralised information systems and thereby fill in information gaps.

  After explicit request from the Council, the High Level Expert Group on information systems and interoperability of the Commission, is invited to undertake activities to determine the implications and to inform the Council of its findings.

- **Create synergy between the risk management of customs**[19] **and information held by JHA agencies**. This will lead to increased interagency cooperation and information-sharing between customs and JHA authorities at Member States and EU level where it concerns the fight against terrorism and serious and organised crime linked to commercial trade. The risk management strategy of the Customs Union encompasses the exchange of information, the analysis of fraud trends and the expertise in the field of customs cooperation with police and border guards. These are pre-conditions for an efficient customs contribution to security.

---

18 7665/16 JAI 258 ASIM 50 RELEX 239

19 EU Strategy and the Action Plan to improve customs risk management COM(2014) 527

The Action Plan accompanying the customs risk management strategy includes a specific action covering the development of cross-sectoral co-operation arrangements, the improvement of sharing and accessibility of (risk) information, and the involvement of customs in risk and threat assessments. JHA and customs authorities need to cooperate in order to achieve the deliverables of this specific action in the timeframe stipulated.

- **Start a longer-term initiative - primarily by assessing the needs of Member States and EU agencies - to develop a coherent approach to the sharing of information with third countries and organisations,** taking fully into account fundamental rights and the provisions of the general EU data protection legislation and specific data protection regimes at EU agencies. Collecting, sharing and connecting information exceeds EU capabilities and should be reinforced with third countries and international organisations considering the challenges in the JHA area.

  The EU JHA Heads of agencies are invited to look together with Governing Bodies of their agencies in which Member States and the Commission take part, into the elements on the basis of which this initiative can be initiated and inform COSI. Afterwards COSI should take the initiative forward considering Member States competences.

4. Way forward

The Roadmap and accompanying action will be centrally and strategically monitored by the Standing Committee on Operational Cooperation on Internal Security (COSI). The dedicated actions will be monitored by the respective dedicated Council fora (e.g. SCIFA, the Terrorism Working Party, the Working Party on Data Protection and Information, the Frontiers Working Party, the SIS/SIRENE Working Party, the Working Party on Cooperation in Criminal Matters and the Customs Cooperation Working Party), the Commission fora and the governing bodies of EU agencies as set out in the action plans, which will report regularly to COSI. The monitoring will fully take into account the competences and responsibilities of the Commission to monitor and follow-up the implementation of EU legislation.

The High Level Expert Group on information systems and interoperability, which the Commission will set up, is invited to propose legal, technical, financial, and operational requirements to pursue interoperability solutions for information systems. Following the findings of the Expert Group the Commission will present further specific ideas to the Council and the European Parliament on ways forward which would also support the implementation, review and adaptation of the Roadmap.

Each year COSI will comprehensively determine the progress in implementing the Roadmap and the accompanying action plans, identify key obstacles and propose a way forward and - where appropriate - seek political guidance from Council. The other fora will undertake these steps and inform COSI with a view to the fulfilment by the latter of its monitoring role.

CHAPTER 2: INFORMATION MANAGEMENT AND EXCHANGE IN THE AREA OF LAW ENFORCEMENT INCLUDING JUDICIAL COOPERATION IN CRIMINAL MATTERS

Theme 1 Information-centred approach to Law Enforcement

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
1	Identify - operational and legal obstacles in order to improve the **availability** of information and the subsequent follow up	Undertake a gap and needs analysis among Member States law enforcement authorities and including public prosecution, EU JHA agencies and customs authorities from a legal, operational, behavioural and (IT) system/technical point of view on the availability of information in existing and pursued EU information instruments to identify redundancies and blind spots. This analysis should include an in-depth evaluation of the factual operational and legal obstacles (including the way principles are applied) and challenges in order to improve the follow-up to information exchange in law enforcement and criminal justice systems and to look at possible bridges with border management systems. *No legal changes required (the follow-up possibly)*	Commission (High Level Expert Group) Member States	Europol Eurojust Frontex eu-LISA FRA	2017	COSI	Commission Budget (not EU funding programmes)

Additional remarks: The complexity of current law enforcement challenges and consequently of multiple and evolving tasks for practitioners has an impact on the need to obtain and analyse/check information. Consequently, this may lead to a need for broader direct access to data in the migration domain or greater efficiency in information sharing between migration and law enforcement domain. In addition extending access rights to a particular system could limit the need for storing information in other systems, thereby avoiding redundancies and consequently having data protection benefits. A number of obstacles have been identified in the recent past and highlighted at various Council levels. Taking such action would be an attempt to complete the picture by ensuring that all possible gaps are addressed.

See Council conclusions following the Commission Communication on the European Information Exchange Model (EIXM) of 6 and 7 June 2013 (9811/13).

The collection, check and connection of information should lead to follow-up operational actions such as post-hit actions, investigative steps, control actions, identification of persons or financial flows, and other actions. These phases cannot be distinguished easily. However, the prerequisite for all those phases is sufficient clear-cut information (including supplementary information) in order to determine which action to undertake. This is vital to ensure proper use of limited resources and to avoid misguided or ineffective actions. A number of obstacles have been defined in the recent past and highlighted by various Council fora. This action would try to complete the picture in ensuring that all possible gaps are addressed.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
2	Enhance data / information quality	A) Within the relevant governing body/working party propose, discuss and agree on a common set of standards (law enforcement, authorities, public prosecution) (inserting and querying data) regarding the quality of data / information B) eu-LISA to develop a central monitoring capacity for data quality. C) Disseminate data quality standards with the help of joint manuals, best practices and expertise among Member States; eu-LISA to share expertise regarding the central monitoring capacity for data quality with Member States and other EU JHA agencies while fully taking into account the prerogatives of Member States and other EU JHA agencies to determine their quality of information monitoring. *A&B: Possibly require legal changes/steps, C: No legal changes required*	Member States Europol, Eurojust, Frontex, eu-LISA	Commission	A&C) 2018 B) 2018/2019 or earlier depending on need for legal changes to the mandate of eu-LISA	DAPIX WP COPEN WP SIS/SIRENE WP Governing Bodies EU agencies	A & C) ISF B) eu-LISA budget – through extra financial support EU budget

Additional remarks: See Chapter 1.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
3	Full compliance with data protection and data security requirements	A) Analyse, develop and promote privacy-by-design solutions B) Share experiences, practices and insights with a view to implementing the EU data protection package *No legal changes required*	Member States Commission eu-LISA	Europol, Eurojust, Frontex,	2017/2018 legally and 2018 -2020 operational processes, awareness.	DAPIX WP	ISF

Additional remarks: Full compliance with fundamental rights and data protection rules is a precondition for managing and sharing information for law enforcement. On 28 April 2016, the EU data protection package was formally adopted by the co-legislators. It now has to be implemented and will require measures to ensure clarity, guidance and workable solutions for the day-to-day work of practitioners. Sharing expertise, experiences and practices internationally will facilitate a practical and more uniform support for practitioners when implementing and applying data protection requirements.

Theme 2 Practitioner centred approach to information management and information exchange

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
4	Pursue interoperability solutions, creating but not necessarily ending with a one-stop-shop information solutions at national and European level through single interface solutions for Member States in view of feeding and searching national, European (e.g. SIS) and international (e.g. Interpol) information systems	A) Provide standardised operational requirements - such as minimum requirements for a user-friendly interface providing standardised structures for data, efficiency and operational gains - enabling tailor-made national solutions and respecting access rights; and provide best practices of solutions (an example of a solutions for access to Interpol's and national systems: Interpol's FIND and MIND[20] solutions, and an example to search Europol's EIS, the index of AWF and national systems: the Europol supported pilot project QUEST). B) Study the best practices in Member States for providing real-time mobile access for practitioners to certain information sources, generation of location-aware signals and alerts and capabilities to provide real-time information, including live audio and video *Sub-action A&B do not require legal changes. However if technical requirements are embedded in legal texts amendments could be required.*	eu-LISA Member States Commission	Europol Eurojust Frontex Interpol	A&B) 2018 following gap analysis action 1	DAPIX WP Expert Group on Information Systems and Interoperability	ISF

[20] Fixed Interpol Networked Database (FIND) and the Mobile Interpol Networked Database (MIND), aim to facilitate simultaneous searches in the Interpol systems and in national systems (including NSIS)

Additional remarks: An easy supply of information and feeding of databases as well as an easy simultaneous access to various systems via one interface – a one-stop-information-shop approach - is vital to increase information sharing and follow-up to information shared. In that context, it is important to note the need for compatibility with / adaptability of such an interface in relation to not only international and European systems but also to national systems. Moreover, existing initiatives in this respect should be taken into account, such as the development of the Universal Messaging Format (UMF).

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
5	Further develop the Universal Messaging Format (UMF	Further develop the Universal Messaging Format The further development of the format should take into account structures and developments of existing information systems such as SIS, while further development of those systems should take into account the UMF. *Depending on the national and European legal framework implementing the UMF will require legal changes.*	Member States Europol Frontex eu-LISA Interpol	Commission	Ongoing (pilots started in 2016 at Europol and in several MS - UMF3 project)	DAPIX WP	ISF financed UMF 3 project

Additional remarks: The UMF Interoperability Coordination Programme aims at producing a commonly recognised standard specification for the exchange of information between national law enforcement authorities. It will ensure semantic interoperability whereby data quality will be strengthened. The programme is to be realised in three phases and two phases have already shown results: 1) definition of a comprehensive European Police Information Model (EU-PIM), which will integrate the current police information models in European Member States and central institutions; 2) based on the EU-PIM, development of the technical specifications for a Universal Message Format. A common technical standard for implementation in IT systems is available. In 2016, the third phase (UMF3) has started and aims at providing the concept and proposal for a management entity and a governance process for the maintenance and development of the new standard. All relevant actors, including law enforcement authorities, should be encouraged to consistently use the UMF standard in order to facilitate cross-border communication.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
6	Increase the trust among and expertise of practitioners at various and between various levels including understanding of each other's practices and backgrounds.	A) (Further) develop national training and awareness raising programmes for law enforcement and public prosecution, including joint training, in cooperation with relevant EU agencies, taking into account all existing channels and tools with their purposes, conditions and benefits. B) Develop cross-border exchange programmes with various categories of practitioners from various levels. The primary focus should lie on the integrated use of those tools while national legal, operational and technical differences should be fully taken into account. An important starting point is the Manual on Law Enforcement Information Exchange as a tool for SPOC personnel[21]. The manual was adopted in 2015 and is regularly updated.[22] Practitioners including from SPOCs, PCCC's and other should be involved in developing and applying the mentioned programmes. *A&B: No legal changes required*	Member States Cepol EJN eu-LISA SIRENE Bureaux	Europol Eurojust Commission Interpol	Ongoing	DAPIX WP LEWP CCWP	A&B) ISF central budget and national programmes Cepol and eu-LISA as EU agencies are not recipients of EU funding programmes. Their assistance requires sufficient means through the regular budget lines for those agencies.

Additional remarks: Cepol already provides various training courses related to the matter which could provide a basis while in relation to a training approach for European law enforcement cooperation, elements can be found in the Commission Communication establishing a European Law Enforcement Training Scheme (COM(2013) 172). Cepol and the European Judicial Network provide exchange programmes which could be a basis for intensified and/or enlarged initiatives or inspire bilateral /trilateral exchange programmes.

[21] see action 7
[22] 6704/16

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
7	Cross border law enforcement cooperation	A) Fully introduce Single Points of Contact (SPOCs) for cross-border law enforcement information exchange in all Member States - including 24/7 availability in relation to Article 7 of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism - based on the guidelines 10492/14 and the SPOC Guidelines for international law enforcement information exchange 6721/14. B) In accordance with the Information Management Strategy action develop training and exchange programmes for SPOC personnel. C) Study the feasibility of Computer Aided Translation to reduce both the information exchange lag and the burden on the staff in SPOCs. D) Develop/introduce effective case management and workflow solutions specifically for SPOCs with a view to mutual legal assistance cooperation. Such solutions require tailor-made elements to fulfil national demands and this initiative should only provide assistance. Hence using (specific) solutions cannot be binding. E) Consider the establishment of common platform (Working Party within the Council or Support group to DAPIX) in order to carry out regular meetings between the Heads of SPOC to discuss up-to-date issues. *A- E: no legal changes required.*	Member States Cepol	Europol Eurojust European Commission (OLAF, DG TAXUD) eu-LISA	A) Ongoing – completion in 2018 B) Ongoing – completion in 2018 C) 2018 D) Ongoing, E) 2018	DAPIX WP COPEN WP LEWP	A. n.a. **B.** ISF central funding. Cepol as a EU agency is not recipient of EU funding programmes. C. EU funding D. EU funding E. n.a.

Additional remarks: The Council confirmed in its Conclusions of 6 and 7 June 2013 following the Commission Communication on the European Information Exchange Model (EIXM) (9811/13) the need to establish Single Points of Contact (SPOCs) for cross-border law enforcement information exchange in all Member States. To that end guidelines were established in document 10492/14. The implementation of SPOCs in Member States should be further pursued according to these guidelines, bearing in mind legal, operational, procedural and other differences between Member States. Thereby rapidity, more coherence and oversight in view of sharing information for mutual legal assistance can be ensured. This will be supported through the implementation of effective case management and workflow solutions. Such solutions require tailor-made elements to fulfil national demands and this initiative should only provide assistance. Hence the use of (specific) solutions cannot be binding.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
8	Enhance bilateral law enforcement information exchange	Strengthen Police and Customs Cooperation Centres (PCCCs) and their cooperation with SPOCs while ensuring a centralised (national or at least state level) overview and monitoring of cross-border information exchange. *No legal changes required*	Member States	Europol Frontex	Ongoing	DAPIX WP CCWP	ISF funded project

Additional remarks: more than forty Police and Customs Cooperation Centres (PCCCs) exist in the EU. They are important instruments for criminal investigation and prevention in border regions and aim primarily at swift and easy cross-border information exchange. They should be strengthened to ensure they are well equipped and up to the task considering quickly evolving security risks.

Theme 3 Optimal use of European information systems

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
9	Improve the information potential of EU agencies	Increase the data supply to Europol and Eurojust as well as systematic sharing of cases as appropriate *No legal changes required*	Member States	Europol Eurojust	Ongoing	MB Europol College of Eurojust	n.a.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
10	Europol to fully use SIS, VIS and EURODAC	A) Europol to fully use its current permission to access to SIS, VIS and EURODAC including by establishing technical effective connections; and B) After undertaking these steps identifying possible obstacles to batch cross-matching on these systems, and keep statistics and provide analysis of use of the above-mentioned databases in similar way as Member States are obliged to do. *A&B: No legal changes required*	Europol Commission eu LISA	Member States	Ongoing, - completion action A in 2017	MB Europol MB eu-LISA WG on Information Systems and Interoperability	Europol budget

Additional remarks: The EU has granted Europol access to the main central databases, but the Agency has not yet made full use of this opportunity. Europol has the right to access and search directly data entered into SIS for arrests, for discreet and specific check and for objects for seizure. So far, Europol has carried out only a relatively limited number of searches in SIS but endeavours to implement a batch search solution to cross-check in particular data received from Third Parties against Europol databases within the current legal framework while a dialogue with the Joint Supervisory Body on data protection matters is required. Access to the VIS for consultation has been legally possible for Europol since September 2013. Since July 2015 the legal basis of EURODAC has allowed access by Europol. The Agency should accelerate the on-going work to establish the connection to VIS and EURODAC.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
11	Enhance the effectiveness of using the Schengen Information System (SIS)	A) Law enforcement, border guard authorities and immigration services include when available identifiers in alerts (copy passport, digital photo, biometrics, DNA-profiles to be considered) on the basis of existing legal provisions; enable searches on fingerprints and provision of facial image feedback in the case of a hit. The workload for SIRENE Bureaux and other practitioners should be assessed when further pursuing this action including through solutions to interpret information easily. B) Implement an Automated Fingerprint Identification System (AFIS) functionality in the SIS within the central as well as national system in view of its full use. C) Find a short term solution to allow reciprocal sharing of information between Schengen, non-Schengen States and Member States who are partially using the Schengen acquis instruments associated to Schengen, pending a permanent solution to this issue in terms of provision and access to EU information databases *A – C no legal changes required*	Member States Commission eu-LISA	Europol Eurojust Frontex SIRENE Bureaux	A) Gradual ongoing process depending on national availability and possibilities. B) 2017 (central level) / 2018 onward (national level) C) 2017/2018	A) SIS/SIRENE WP B) MB eu-LISA SIS/VIS Committee C) SIS/SIRENE WP SIS/VIS Committee	A) n.a. B) Introduction in central system - EU budget Introduction nationally – national budget (with after 2017 possibly ISF funding) C) to be determined

Additional remarks: better identification of persons in the event of a hit will be possible by the uploading of additional information with the alert when it is available. These can be various indicators such as biometric data, warning markers or (digital) photographs. Also searching on fingerprints by means of an AFIS (Automated Fingerprint Identification System) to be implemented in the SIS will speed up identification and make it more reliable. These identifiers should be added to the alerts if they are available. The absence of identifiers should, however, not make it impossible to insert an alert. Member States will improve national processes to enforce the addition of such identifiers with an alert.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
12	Enhance the effectiveness of using the Schengen Information System (SIS)	Revise the legal basis of the Schengen Information System taking into account the evaluation undertaking by the Commission (including new functionalities, extend the access of EU agencies while fully taking into account the information owner principle and the legal base of the agencies, facilitating access to hit information). The revision should include the provision for a long-term solution to allow the reciprocal exchange of information between Schengen, non-Schengen Member States and Member States who are partially using the instruments associated with Schengen Further explore and decide if MS return orders can and should be inserted in SIS. *Legal changes required*	Commission Council European Parliament	eu-LISA Europol Eurojust Frontex	Ongoing: Proposal end 2016 Adoption co-legislators 2017	Schengen Working Party (SIS/SIRENE) configuration	EU funding in view of implementation

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
13	Full use of Prüm possibilities to exchange fingerprints, dna and vehicle registration data	A) Undertake EU pilots and if required follow-up steps to enforce connections of Member States to the Prüm network. B) Identify key obstacles for: i: the connection to the Prüm network ii: the full use of Prüm possibilities iii: solve the obstacles C) Examine the possibility for Europol to become a partner in the Prüm framework with a view to enabling the cross matching of DNA, finger prints and vehicle registration data with third countries with which Europol has an operational agreement while fully taking the information owner principle into account. *A&B: No legal changes required, C: legal changes required*	A) Commission B) Member States, Commission C) Commission	Europol Eurojust Frontex	A) Ongoing, B) Ongoing C) 2018	Commission DAPIX WP	A&B (i and ii) Not applicable B (iii): ISF funding national programmes C n.a.

Additional remarks: DNA, fingerprints and vehicle registration data are key identifiers in criminal investigations and possibly provide evidence for criminal proceedings. In view of the ever increasing international dimension of organised crime, terrorism and other security risks, it is vital that all Member States are as soon as possible fully connected to the Prüm automated data exchange. Moreover, Member States should prioritise operational connections with other Member States. Implementation obstacles should be addressed as soon as possible.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request Ffnancial support
14	Improve the sharing of criminal records, particularly relating to terrorism convictions	A) Facilitate access to ECRIS for all relevant authorities and increase use of the system B) Additionally, consider solutions (other than the ECRIS system) to allow the pro-active sharing of convictions data, in particular relating to terrorism; and, as appropriate, assess the legal and practical feasibility of implement a solution which includes making certain convictions data available to the relevant authorities. *A: No legal changes required, B: Legal changes required*	Member States Eurojust Commission	Europol Frontex OLAF eu-LISA	A) Ongoing B) 2019	COPEN	A) n.a. B) to be determined

Additional remarks: Member States should invest in facilitating the access to ECRIS at national level to ensure the increased use of ECRIS. In urgent cases, Member States should reach out to Eurojust to facilitate the obtaining of criminal records. When the access has not yet been established Member States should exchange information on the basis of Framework Decision 2009/315/JHA. After the adoption of the legislative proposal on the complementation of ECRIS with an index system to enable national authorities to determine which Member State holds criminal records of a third-country national, Member States are invited to make full use of this possibility.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
15	Enhance the coordination and monitoring capabilities of Eurojust Members	Enable the setting up and connection of the members of the Eurojust National Coordination System (ENCS) to the Eurojust's Case Management System (CMS) *No legal changes required*	Member States Eurojust	Europol Frontex OLAF	Ongoing in view of completion in 2017/2018	College of Eurojust	EU funding

Additional remarks: the Case Management System (CMS) is designed to store and process case-related data referred to Eurojust for assistance. To improve its functionality and operational performance, two upgraded versions of the CMS were released in 2015 to support implementing the connection of members of the ENCS from each Member State to the CMS, as envisaged by Article 12 of the Eurojust Council Decision. Secure network connections have been set up with a number of Member States, ensuring the secure exchange of information between Eurojust and the Member States. The added value of well-functioning Eurojust National Coordination Systems (ENCS) has become particularly evident in the field of counter-terrorism.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
16	Streamlining and speeding up international information exchange by automation of manual procedures	Develop the Automation of Data Exchange Process (ADEP) project The project must ensure complementarity with existing information management solutions especially with regard to Europol (EIS), as well as seek a low-cost, legally proof and user-friendly solution. *Legal changes possibly required particular when implementing*	Member States	Europol	Ongoing in accordance with the current IMS project.	DAPIX WP	ISF funded project

Additional remarks: rapid and efficient information exchange is essential to ensure fast follow-up actions in investigations, control actions and other activities. Hence it is important to determine swiftly where vital information is present and to address oneself to the right party. The Automation of Data Exchange Process (ADEP) aims at addressing this need and thereby providing a contribution to the goals of Council Framework Decision 2006/960/JHA (SFD). The technical development of ADEP takes into account Annex A on categories of offences of Decision 2009/316/JHA (ECRIS).

CHAPTER 3: STRENGTHEN THE COLLECTION, CHECKING AND CONNECTION OF INFORMATION FOR THE DETECTION OF PERSONS INVOLVED IN TERRORISM AND TERRORISM RELATED ACTIVITY AND THEIR TRAVEL MOVEMENTS

Theme 1 Improving existing instruments – quantity, quality and timeliness

SIS

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
17	Create a joint understanding of when a person should be entered in the SIS regarding terrorism and terrorism related activity	Agree on indicative criteria for inserting terrorism related SIS alerts	Member States, TWP, SIS VIS Committee	MS (SIRENE Bureau) eu-LISA	2016, ongoing	COSI	n/a

Additional remarks: SIS already is a valuable tool, common criteria to define whether a person is involved in terrorism or terrorism related activity in the Member States will be of added value. This will positively affect the upload of alerts in the SIS and action by end users on a hit. Differences in national procedures for adding 'terrorism related activity' as a type of offence make it difficult to establish any clear typology for these individuals. The definition of terrorism in the revised Council Framework Decision 2002/475/JHA provides guidance for further efforts to come to more harmonised applications. In order to provide clear expectations as regards actions to be taken and the necessary response with regard to SIS alerts and information sharing, indicative criteria are set regarding the exchange and sharing of information on individuals attracted to areas of conflict, whether to fight or to support terrorist groups. This action is related to action 20.

The Group of Most Affected Member States previously agreed on a list of criteria in an Annex to the Milan conclusions of July 7th 2014 (see annex).[23] Indicative criteria will be agreed upon on the basis of this list as well as up-to-date information and other indicators such as the common risk indicators for the performance of border checks (as developed by Frontex and the Dumas Working Group).

These criteria can also be taken into consideration for the sharing of information with Europol, for example with the Europol Information System and the Focal Point Travellers. This action is closely connected with action 24with regard to the (quality) of information given with an alert via the M-form.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
18	Ensure structural information to SIRENE Bureaux and SIS end users on persons involved of terrorism or terrorism related activity	Member States will create alerts once criteria are met (unless there are operational reasons not to)	Member States	SIRENE Bureaux	2016, ongoing	COSI	n/a

Additional remarks: alerts on persons are made on the basis of the indicative criteria developed under action 1. Member States need to use the criteria to determine whether an alert should be entered. While these criteria are not legally binding and are non limitative, meeting only one of the criteria listed should lead to the insertion of an alert unless a Member State determines that an exception must be made. Any transmission and sharing of information about the persons referred to remains, of course, subject to safeguards provided for in national and European law. Member States will ensure due consideration is given when an alert after meeting the criteria is not inserted. Member States will share insights into interpretations of legal standards or national operational practices to strengthen mutual understandings and possible good practices. This actions relates to action 17.

[23] In addition to the Milan Conclusions, see UN Resolution 2178, Council Framework Decision 2002/475/JHA, Council Framework Decision 2008/919/JHA and SIS code tables (ST 028 terrorism related activity).

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
19	Ensure clear indication to SIRENE Bureaus and SIS end users that an alert concerns a person involved of terrorism or terrorism related activity	Use of marker 'terrorism related activity' where applicable	Member States	SIS VIS Committee, SIRENE Bureaux eu-LISA	2016, ongoing	COSI	n/a

Additional remarks: the marker 'terrorism related activity' is added with an alert issued on persons to whom this marker is applicable. The default setting will be that when discreet or specific check alert under Article 36 SIS II Decision an Article 36 alert is entered on a person involved in terrorism or terrorism-related activity the marker 'terrorism related activity' is always added to the alert, when immediate action is required. By using the marker as a default, clarity and consistency in practice can be ensured. In addition to issuing an alert on a person based on the criteria, the use of the marker will provide SIRENE Bureau and end-users with even more insight and assurance as to what is expected of the actions based on the alert. Member States will ensure due (operational) consideration is given when this maker is not added to the alert. Any transmission and sharing of information about the persons referred to, remains of course subject to safeguards provided for in national and European law.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
20	Ensure sufficient quality of data in SIS, so that informed follow up actions can be taken	Minimum standards for data quality required by SIS should be respected by Member States	Member States, SIS/SIRENE, EC, SIS-VIS Committee	eu-LISA SIRENE Bureaux	2017, ongoing	COSI, eu-LISA	n/a

Additional remarks: Member State authorities need insight into the validity/reliability of information, which is shared in order to follow up effectively after a hit. The absence of common standards between Member States diminishes the impact of information sharing and follow-up actions. This is valid for information uploaded in the Schengen Information System (SIS) and in the Europol Information System (EIS) as well as for information shared with Europol's Focal Point Travellers and Hydra. Member States commit themselves to respecting the commonly agreed operational and technical requirements regarding data quality. Regular discussions will be held, detailing, for example, the importance and the exact purpose of data provided and received, of data transfer in a commonly agreed language, and of enabling prioritising actions. Technical solutions in the SIS to support compliance are explored and implemented by eu-LISA with a view to providing regular feedback to Member States on data quality. High level abstract reports will be sent to the Commission. A special SIRENE form should be developed for the exchange of supplementary information including predefined multiple choice fields. In the meantime Member States should provide in the M-form at least minimum information on the reasons and circumstances governing the sharing of information. Simply sending an almost empty form does not match the operational needs. This will be added to the existing predefined fields and free text areas and they should be filled in to be able to finalise the M-form. Regarding the systems under the competence of eu-LISA, these actions are covered by the action plan on information management and exchange in the area of law enforcement.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
21	Ensure additional information on criminal records is available to SIRENE Bureaus and SIS end users	Insert additional informationbased on criminal records (national databases and ECRIS) with an alert	Member States, SIS VIS Committee	Eurojust, SIRENE Bureaux, EC	2016, ongoing	COSI	n/a

Additional remarks: information pertaining to the criminal records of a person for whom an alert is entered in the SIS is uploaded with the alert, when available and relevant. The use of information from the ECRIS when issuing SIS alerts, especially also in cases of 'terrorism-related activity', can provide valuable background information to the SIRENE Bureau and the end-users.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
22	Create a joint understanding on immediate reporting upon a hit in the SIS	Commonly define when 'immediate reporting' is required upon a hit as well as what action should be taken	TWP, SIS/SIRENE WG	SIRENE Bureaux Commission, eu-LISA	2016, ongoing	COSI	n/a

Additional remarks: the nature of some articles such as Articles 24 of the SIS II Regulation, 36 and 38 of the SIS II Decision leave room for differences as regards the interpretation of the action taken in response to a hit. For example, persons subject to a nationally imposed travel ban will perhaps not be stopped based on an Article 36 alert even though they are in violation of their travel ban. The confiscation of documents pursuant to seizure alerts (Article 38 of the SIS II Decision) is not always automatic but may depend upon national legislation.

In addition, the national procedures for adding the requirement for immediate reporting in response to an alert vary greatly. Time is a crucial element; therefore authorities need clarity on why immediate reporting is required, and what the actions look like. To ensure harmonised use and understanding, the criteria for using the new 'immediate reporting' option will be harmonised and it will be made clear in which cases this option should be used. In this view, a study by the Commission (or eu-LISA) to indicate the outcome in cases of "immediate reporting" is required. The M-form should contain further information that can be immediately given to the officer in the field. Contact with the competent SIRENE Bureaux should be made without delay, for example by telephone. The SIRENE Manual will be amended to set commonly agreed desired interventions and to support compliance. To act properly, training of the end users is essential. Further specifications to strengthen the practice for specific articles will be taken up where appropriate for that article.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
23	Make possible that SIS alerts can call for preliminary and temporary holding or detention where sufficient national legal grounds are available	Create a new type of action	Commission (EC), SIS/SIRENE WG	Member States	2017-2018, ongoing (update SIS II Regulation and Decision)	COSI	n/a

Additional remarks: The current possibilities for action after a hit following an alerts based on articles pursuant the SIS II Regulation and Decision, do not fully meet the operational needs. For example, the nature of Article 36 SIS II Decision allows for no types of action other than discreet or specific checks. Often there is no European Arrest Warrant yet for a person who is the subject of an alert for terrorism-related activities under Article 36 SIS II Decision, although after a hit more action can be needed than a discreet or specific check. An example would be persons subject to a national travel ban. Therefore, whilst maintaining the possibilities provided by the existing alerts within the SIS legal framework, a new type of action should provide for the possibility of preliminary and temporary holding or detention, where sufficient national legal grounds are available.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
24	Ensure that end users are equipped to conduct discreet and (where national legal ground are available) specific checks	Strengthen effective discreet and specific checks including through training the trainers	EC, Member States, CEPOL, eu-LISA	SIRENE Bureaux	2016 (start), ongoing	COSI	n/a

Additional remarks: Carrying out a discreet check is also a matter of proper information and training, f.e. train the trainer. Specifically, when it comes to alert with the marker 'terrorism related activity'. To enable better support for the end-users the M-form must be filled in with specific information, such as warning markers. Training activities for end-users including with the support of CEPOL and technical support should facilitate Member States in carrying out a discreet or specific check.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
25	Systematic feedback on hits or requests for immediate action to national SIRENE Bureaux and the issuer of an alert	Enable systematic reporting of a hit in SIS to the national SIRENE Bureaux of the Member State where the hit occurs as well as the Member State that issued the alert	SIS VIS Committee, EC, Europol, Member States	SIRENE Bureaux	2017, ongoing	COSI	n/a

Additional remarks: Real time notifications of the SIRENE Bureaux if a terrorism related alert is consulted does not always take place; this is particularly necessary for alerts for which immediate reporting is required and alerts concerning 'terrorism-related activity'. This also applies to any supplementary information obtained during the exchange of information.

Specifically after major incidents, the diffusion of information to other Member States is vital. The occurrence of a hit should therefore be immediately and automatically reported to the national SIRENE Bureaux that issued the alert.

Member State good practices and technical support enabling information to become directly available to the end-user and the SIRENE Bureau, should be explored as a solution to this action. Member States will consider the possibility of systematic transmission of hits – and accompanying information - to Europol, for example to the Focal Point Travellers or Focal Point Hydra. Systematic diffusion of hit information to Europol may require legal amendments, thus necessitating legal analyses.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
26	Ensure that information of extremist speakers, who are deemed to pose a threat to public order, is shared between Member States	Make optimal use of SIS, primarily through Article 24.3, and in accordance with national legislation, where appropriate issue alerts for third country nationals who are not present on the territory of MS	EC, co-legislators, follow-up Member States	Member States (e.g. SIRENE Bureaux)	2017, ongoing	COSI	n/a

Additional remarks: Member States agree to flag all extremist speakers with or without visa obligations, who are deemed to pose a threat to public order and who intend to visit the EU, in SIS under the appropriate article. This allows Member States to take notice of the extremist speakers that other Member States have identified, and take the necessary measures. An alert in SIS is necessary to ensure that an assessment is performed every time an extremist speaker, who is deemed to pose a threat to public order by a Member State, intends to visit the EU. Member States will flag extremist speakers for a maximum of two years and alerts will be removed or continued if deemed appropriate, based on a continuous assessment. Member States may consider to adjust national legislation to accommodate the objective.

N	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
27	Ensure that both law enforcement authorities and security services can quickly enter alerts into the SIS	Where necessary, change national practice to ensure that both law enforcement authorities and security services can insert alerts in the SIS directly without interference of judicial authorities	Member States	Member States' SIRENE Bureaux TWP, SIS SIRENE	2016, ongoing	COSI	n/a

Additional remarks: Member States will ensure that law enforcement authorities and security services (alerts under Article 36) have the possibility of entering alerts into the SIS without interference of judicial authorities. Good practices which facilitate the involvement of law enforcement authorities and security services in making use of SIS (including secondment to the SIRENE Bureau) and removal of legal/administrative obstacles at the national level will be shared.

Stolen and Lost Travel Documents database

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
28	Allow checks against travel documents that have not yet been declared stolen, lost or invalidated	Insert documents associated to alerts on persons into the Interpol TDAWN when deemed necessary	Member States, third countries, Interpol	eu-LISA	2016, ongoing	COSI	n/a

Additional remarks: Member States face challenges inserting alerts on travel documents in the SIS or the SLTD, when these document haven not yet been declared stolen, lost or invalidated for travel purposes. Therefore, TDAWN should be available in combination with Interpol diffusions. Member States will consider entering travel documents associated with persons they have signalled in the SIS into TDAWN and Interpol diffusions, when deemed necessary as well (provided that Interpol can respect the restricted diffusion when using TDAWN). Further support for these actions can be found in the action plan the Commission will present on preventing and detecting document fraud for EU and non-EU passport and travel documents as soon as possible.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
29	Full connectivity to SLTD at external border crossings	Make the SLTD nationally available for automated and systematic checks	Member States	Interpol	2017, ongoing	COSI	

Additional remarks: Member States should establish electronic connections to SLTD during checks and establish these connections to all end-users, especially at their external border crossings and at visa-issuing consulates Further support for these actions can be found in the action plan the Commission will present on preventing and detecting document fraud for EU and non-EU passport and travel documents as soon as possible.

Europol

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request
30	Ensure that information on FTF is consistently and systematically uploaded to European systems and platforms, and synchronised where possible	Implement a consistent three-tier information sharing approach regarding FTF by making optimal and consistent use of SIS, the Europol Information System (EIS) and the relevant Focal Points at Europol	Member States, Europol	SIRENE Bureaux eu-LISA	2017, ongoing	COSI	n/a

Additional remarks: Member States should consistently and systematically upload information on Foreign Terrorist Fighters to the European systems and platforms. While any transmission of information remains submitted to safeguards provided in national and European law, Member States will ensure due consideration is given when information is not uploaded to any of these systems out of operational reasons.

The EIS is used as a database to consistently store information on Foreign Terrorist Fighters and complementary information which is not available via the SIS. Terrorism related information in the SIS and EIS should be synchronised wherever possible in order to ensure consistent data quality. Since this is not an automated process, the responsibility lies with the data owner. Member States should consider to share relevant SIS hits on foreign terrorist fighters via EIS following the 'Three-tier approach'. The EIS in this case (as a 'memory of hit') would contribute to filling information gaps. Several Member States have already put this approach into practice by e.g. indicating in EIS that based on SIS hit Person A who is subject to a discreet check crossed the border between Member State A and Country B on 10.04.2016, in vehicle reg. number XXXXX, registered in Member State C. Person B was also in the vehicle. A technical (automated) solution at the European level could be explored to support this process.

The EIS should be available to all competent counter-terrorism authorities of the EU and its Member States and be fully used by them; a data loader will be beneficial. There is another way of uploading a large amount of data using so called batch upload. If applicable, reference to SIS II alerts should be made when entering data in the EIS.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
31	Ensure better use of existing secure channels for exchange of information regarding terrorism and terrorism related activity	A) Make better use of SIENA as a secure channel for the exchange of law enforcement information regarding terrorism and terrorism related activity, B) Consider introducing a 24/7 regime of work in order to improve the effectiveness of channels	Member States, Europol	TWP	A: 2016 B: 2017 (discussion) - onward (national implementation)	COSI	n/a

Additional remarks: Europol continues to promote the further roll-out of SIENA to law enforcement authorities in Member States. End 2015, Europol has created the possibility for counter-terrorism units to communicate bilaterally via SIENA. Currently, Europol is working on the upgrade of SIENA to CONFIDENTIAL UE/EU CONFIDENTIAL – this features is expected to be available in the course of 2016. In 2016 and 2017 the functionality of the SIENA web service will be extended, offering better possibilities for integration with national systems.

Eurojust

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
32	Ensure that Member States are informed on all prosecutions and convictions on terrorist offences in the EU	Transmit to Eurojust information on all prosecutions and convictions on terrorist offences	Member States, Eurojust	TWP	2016, ongoing	COSI	n/a

Additional remarks: As required by Council Decision 2005/671/JHA, Member States should transmit to Eurojust information on all ongoing prosecutions and convictions for terrorist offences, as well as information on the specific circumstances surrounding those offences, links to other relevant cases, Mutual Legal Assistance (MLA) requests and information on the execution of such requests. This allows Member States to benefit from Eurojust' s capabilities to detect links between cases, as well as from Eurojust' s continuing efforts to centralise and analyse challenges and best practice related to prosecutions for terrorist offences shared with the Member States, in particular via the regular Eurojust Terrorism Convictions Monitors (TCM), Eurojust's FTF Reports and Eurojust's contributions to the annual EU Terrorism Situation and Trend Report (TE-SAT). In this regard, Member States are also called upon to exchange with Eurojust information on cases of illicit trafficking in firearms, on drug trafficking, illegal immigrant smuggling, cybercrime, and other serious crimes. This will allow Eurojust to systematically cross-match existing information and establish possible links between terrorism and other serious crimes.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
33	Ensure connection of Eurojust to the Focal Point Hydra at Europol	Connect Eurojust to the Focal Point Hydra at Europol	Eurojust, Europol	Member States	2016, 2017	COSI	n/a

Additional remarks: Eurojust is already successfully connected to the Focal Point Travellers. Member States will support and facilitate the association of Eurojust to Focal Point Hydra to ensure that Eurojust can provide timely and efficient support to the investigations and prosecutions in the Member States.

Theme 2 Organise to protect: connect silos and expertise

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
34	Nationally connect counterterrorism experts and other services involved in the detection of travel movements of persons involved in terrorism and terrorism related activity	At national level – if not existing -, it is advisable to create multidisciplinary platforms on the detection of travel movements of persons involved in terrorism and terrorism related activity	Member States		2016	COSI	n/a

Additional remarks: within the Member States, a large number of actors is involved in the detection of travel movements of persons involved in terrorism and terrorism-related activity. These actors should be connected, for instance through multidisciplinary platforms for the exchange of expertise and discussions of improvements in national processes.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
35	Ensure that national good practices regarding cooperation with third countries on counterterrorism are shared between Member States	Share good practices on cooperation with third partners in relation to counterterrorism among MS and third country partners	Member States, TWP	EC	2017	COSI	

Additional remarks: operational practices can benefit from a clear understanding of current information exchange on terrorists between EU Member States and third countries. This action could include ways in which information received from third countries is entered into the SIS upon request, the use of Interpol diffusions and sharing of watch lists, common risk indicators, also taking the advantage of agreements concluded by Europol with third partners.

	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
36	Ensure common understanding between end users, regarding the detection of travel movements of persons involved in terrorism and terrorism related activity	Create joint and multidisciplinary training for CT, border and law enforcement experts in cooperation with existing expert groups such as SIS/SIRENE, regarding the detection of travel movements of persons involved in terrorism and terrorism related activity	Member States, CEPOL, Frontex	SIS/SIRENE, TWP, SIS VIS Committee	2017	COSI	

Additional remarks: a common understanding of the different roles and practices amongst CT, border and law enforcement experts is a necessary condition for improved information exchange, in particular in terms of quality of information. Therefore joint and multidisciplinary training courses should be created.

Theme 3 National detection capabilities by PIUs

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
37	Ensure compatible national implementation of the PNR-directive in the Member States	Initiate operational PNR informal working group	Presidency, Member States and Commission	PIUs in Member States, Europol.	2016	n/a	Member States

Additional remarks: To ensure consistency in the implementation of the PNR Directive and compatibility of national passenger information units (PIUs), Member States are invited to join in an operational PNR informal working group, initiated by the current Presidency. The group must include the heads of the national PIUs and experts. This group will discuss development of the (future) operational practices of PIUs, within the EU framework, and with Europol and third countries. Shared principles for information exchange will support a harmonised and optimal operational cooperation between the PIUs. Through the group, operational and technical support and facilitation of good practice exchanges could take place.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
38	Use national practice of Member States in the construction of new PIUs	Offer technical assistance in construction of PIUs	Member States		2016	n/a	Member States

Additional remarks: within the operational PNR informal working group, Member States who have already set up their national technical facilities for the PIUs will share, where appropriate, their technology, experiences and expertise to support Member States who have not yet done so. Those Member States which have not yet set up PIUs are encouraged to mobilise their national part of the ISF to do so.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
39	Agreement on how information is shared between PIUs and with third countries where possible	Ensure interoperability and share information on suspects and anomalous travel patterns and targeting rules	Member States, Commission /Europol,		2018	n/a	n/a

Additional remarks: Member State PIUs will agree on the way to share information on suspects and anomalous travel patterns and targeting rules, between the PIUs and with third countries where possible. Interoperability and information exchange between PIUs is key to ensuring an effective use of PNR. The future PIUs need to be interoperable. Lessons learnt from projects such as the FIU.net embedment should be taken into account when developing information exchange infrastructure and practices for the future PIUs to ensure a shared perspective is integrated from the beginning. Member States are encouraged to participate to the maximum extent in the Commission ISF projects on interoperability and other multilateral and international initiatives on this important issue. Europol could be of support in the EU level discussions on targeting rules used at national level, and the development of supranational targeting rules.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring	Council request financial support
40	Make full use of Europol databases to support PIUs	Define Europol support of PIU practices, cooperation, and activities	Member States, Europol,	EC	2017	n/a	n/a

Additional remarks: Following Article 10 of the PNR-directive, Europol plays a role in supporting national PIUs. Europol databases can bring added value to PIUs as a source of additional intelligence (to verify, cross-check, and ensure that informed decisions are taken). As a fundamental principle it should be recognised that operational cooperation and layering of travel information with other sources of intelligence are beneficial for identifying new/additional links/suspects/lines of inquiry. Europol could facilitate ensuring a supranational perspective on travel patterns and targeting rules.

CHAPTER 4: BORDER MANAGEMENT AND MIGRATION

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
41	Registering entry and exit at the EU external borders of Persons enjoying free movement.	Examine the need and added value of registering travel movements of persons enjoying Free Movement of Persons, including an assessment of impact, costs, proportionality of the different possible solutions (including broadening the scope of EES)	COM, High Level Expert Group	Commission, Member States, eu LISA, EDPS, Frontex	End 2016	SCIFA/COSI/WG Frontiers	ISF,

Additional remarks: In response to the security challenges that were highlighted once again by the Paris and Brussels attacks, to equip the EU with rapidly effective and safe tools in order to improve our external border control. It is necessary to assess the need added value of registering the entry and exit of persons enjoying Free Movement of Persons, including for people with the right to circulate freely, making use of modern technology in order to ensure smooth flows. Such an assessment should also include an evaluation of financial and technical viability of the project. The possibility to establish a module or extension within the EES should also be assessed. This assessment shall be a activity not hindering the current negotiations on the EES for third country nationals. See Actions 42 and 44.

24

24 This answers the decision taken by the JHA Council on 25 February 2016.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
42	Registering entry and exit at the EU external borders and admitted for a short stay and refusals of entry of third country nationals including contributing to return.	Negotiations on the legal proposals on Smart Borders, EU Entry and Exit and amendment of the SBC in the Frontiers Working Party	Member States, Commission and EP	eu-LISA	December 2016	SCIFA/COSI/ WP Frontiers	ISF, COM Budget

Additional remarks: In addition to the existing ICT systems the Commission has propose on the 6 April 2016 to establish another centralised IT system, the Entry and Exit system (EES) to improve the external management to reduce irregular immigration by addressing the phenomenon of overstaying and to contribute to the fight against terrorism and serious crime, thereby contributing to a high –level of internal security. This system should be implemented by 2020. (Legislative proposals "Smart Borders" doc 7675/16 and doc 7676/16) See Actions 41 and 44, in this regard action 50 is also of relevance.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
43	Close the information gap on pre-arrival data for travellers not generating API, PNR or visa data	Feasibility study and policy study of an EU Travel Information and Authorisation System	Commission	Commission, Member States, eu-LISA, EDPS, Frontex	October 2016	SCIFA/ WG Frontiers and VISA	ISF, COM budget

Additional remarks: While law enforcement authorities can obtain (pre) information on visa holders from the VIS of necessary for combating of serious crime and terrorism, no comparable data is available on visa-exempt persons. Ongoing visa liberalization processes are likely to lead to a considerable increase of visa-exempt travellers in the near future. In this context the possibilities of an EU electronic system for travel authorization for visa exempt third country nationals should be further examined. Such an "ETIAS" would ensure that all third country nationals intending to travel to the EU – and not only those who are submitted to a visa requirement – could be subject to some form of pre-screening in advance of travelling and could be pre-authorised before arriving at an external border crossing point. This system would allow collecting and checking information about third-country nationals intending to travel to Europe on an individual basis, with a view to grant them authorisation to travel to the EU‟s external borders. Similar systems have already been set up in Australia and the United States (U.S.). Based on experiences in the U.S. and Australia and taking into account pre arrival information systems (Maritime Single Window, PNR and API), an ESTA could be defined as a system for the purpose of:

a) collecting applications for authorisation to travel to their territory for short-term tourism or business stays, directly from foreign nationals and through electronic channels;

b) determining the eligibility of foreign nationals to travel to their territory for short stays without having to go through a full visa application process;

c) determining whether such travel poses any law enforcement or security risk;

d) having a possibility to prevent a foreign national from travelling to their territory if such travel does pose a law enforcement or security risk, while also retaining the possibility to deny a traveler entry at the border even in case he/she has been granted a travel authorisation. In order to allow a formal discussion on the added value of such a system, the feasibility study should explore all options considering the necessity and proportionality of an ETIAS

(Communication "Stronger and Smarter Information Systems for Borders and Security")

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
44	Enhancing of the security check in hotspots	In order to improve both the timing and execution of each security check, each step should be clearly defined in the SOPs of the hotspot and relocation workflow. Access should be provided to the relevant databases SIS, EU VIS, Eurodac, Interpol databases & Europol databases, in particular to facilitate information exchange on security concerns in relocation cases including exchange of fingerprints before relocation. For relocation, a questionnaire should be launched in order to establish when a relocation file meets the right standards. In case of a rejected relocation file because of security concerns, this information should be shared with all MS.	EU agencies & host MS (EL & IT)	Member States, Commission	Immediate	SCIFA/COSI/WG Asylum	ISF, AMF

Additional remarks: The Presidency has formulated the recommendations on security checks in the hotspots and during the relocation process, which were discussed and supported by a large number of Member States during COSI-SCIFA on 18 April 2016. The hotspot workflow starts at the moment of arrival/apprehension, up to the point of onwards movement from the registration centre, or open or closed reception centre. Both the hotspot workflow and the relocation process have to be designed in such a way that the security checks are integrated and take place systematically, without creating new bottlenecks. Next to deciding on asylum, relocation or return, these checks also serve to ensure that the person does not represent a threat to internal/EU security. Access needs to be organized without delay to the SIS, VIS, Eurodac, Interpol and Europol databases to perform appropriate security checks In order to further accelerate the relocation process, COM will launch a questionnaire on the basis of which MS could indicate what constitutes a "quality" relocation file, including "sufficient" information on security aspects. By setting a clearer standard of what information should be included in the relocation file, MS would have fewer reasons to require additional checks which delay the process. In case of rejecting a relocation file, the MS of relocation should motivate the decision to refuse a relocation request based on the grounds foreseen under the Council Decisions 2015/1601 of 22 September 2015 and 2015/1523 of 14 September 2015. If the rejection is related to security concerns about relocation cases, if possible within the national legislation, this information need to be shared as soon as possible with the benefitting Member States.

(EU Council Conclusions of December 2015)

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Financial support
45	Enhance operational cooperation of EU MS on migrant smuggling through their activities in the hotspots.	All agencies need to continue to make the necessary resources available, including for translation and interpretation	Frontex, Europol, Eurojust and EASO	Member States	Immediate	SCIFA/COSI	n/a

All agencies (Frontex, Europol, Eurojust and EASO) need to continue to make the necessary resources available, including for translation and interpretation, to enhance operational cooperation of EU Member States on migrant smuggling through their activities in the hotspots. Whenever possible, also transport to the registration area should take place from centralized disembarkation points on the islands or on the mainland, also with a view on informing migrants as early as possible about relocation, asylum and (voluntary) return, and the risks of onwards irregular migration. Coordinating arrivals in this way results in more control over the hotspot workflow and the relocation process, and counters smuggling activities.

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
46	Increase of the use of API data for border management	Establish systematic cross-checking of API data against SIS and Interpol SLTD database	Member States	Commission, eu-LISA, Frontex and other relevant agencies	End 2017	COSI	ISF

Additional remarks: Technological developments allow in principle to consult relevant databases without delaying the process of crossing the border, as the controls on documents and persons can be carried out in parallel. The use of passenger information received in accordance with Council Directive 2004/82/EC can also contribute to speeding up the process of required controls during the border crossing process. In this context systematic cross-checking of API data against SIS and Interpol SLTD database should be established.

(Communication "Stronger and Smarter Information Systems for Borders and Security" and Evaluation of the COM on the API Directive)

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
47	Strengthen the information position of EU MS on border management(and combating terrorism and organised crime)	Assessment of the need to revise the legal basis of processing of API data	Commission	Member States, Frontex	2017	SCIFA/WG Frontiers	N/a

Additional remarks: To ensure a wider implementation and to include an obligation for MS to require and use API data for all inbound and outbound flights an assessment of the current API legislation is necessary. This is particularly relevant in the context of the implementation of the PNR Directive as a combined use of PNR and API data further enhances the effectiveness of PNR data in combating terrorism and serious crime.

(Communication "Stronger and Smarter Information Systems for Borders and Security" and Evaluation of the COM on the API Directive)

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
48	Enhancing the functionalities of the VIS.	Examination further improvement's of the **VIS** with a possible need for amending the legal base	Commission	eu-LISA Member States, Europol	before end 2016;	SCIFA/WG VISA	n/a

Additional remarks: To further Improving data quality of data entered into the VIS, including improving the quality of facial images to enable biometric matching. To facilitate the checking of Interpol's SLTD database during a visa application and to achieve interoperability with the SIS to search with VISA applicants fingerprints in the future Automated Fingerprint Identification System to be developed for the SIS e.g. to allow search by travel document, as proposed in the EES.

(Communication "Stronger and Smarter Information Systems for Borders and Security")

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
49	Revision of the EURODAC Regulation	Negotiations on the legal proposal on Eurodac	Member States, Commission and EP	eu LISA	End 2017	SCIFA/WG Asylum	n/a

References to other actions in the Roadmap: actions related to the hotspots and actions related to organising by easier access of LEA to IT systems in the field of migration in the general framework of their duties.(Legislative proposal Eurodac of 4 May 2016)

No.	Objective	Action	Primary Responsible Party/Parties	Stakeholders	Timetable	Monitoring-mechanism	Council request financial support
50	To address the existing information gap on the (travel) documents of third-country nationals.	Assessment of the need of central Residence Permits Repository whether such new EU tool is necessary, feasible and proportional to address the existing information gap on these categories of third-country nationals.	COM	Member States, eu-LISA, Frontex	first half of 2017	SCIFA/COSI/WG Frontiers	ISF, eu LISA

Additional remarks: Residence Permits Repository. The issuance of residence permits, residence cards and long stay visa is within the competence of the Member States. However, when holders of these residence permits, residence cards or long stay visas cross the Schengen area external borders, the decentralised management of these documents entails difficulties for border controls. Individuals bearing travel documents issued by third countries have to be checked at the border in a specific way on the basis of documents whose validity and authenticity cannot be verified against a common database. Even though it is possible to establish through a biometric verification that the traveller is the legitimate bearer of a residence permit, this is not the case for the residence cards and long term visa as no common format exists. This situation constitutes of a security risk that should be addressed.

In addition to security considerations, there is also the aspect of facilitation of border crossings: third country nationals who are exempted from short-stay conditions will not be covered by the scope of the EES(in the current proposal). The introduction of EES will allow third country national short-stay visitors to benefit from automated border crossing solutions such as eGates, but this possibility will not exist for third country nationals with long term right of stay. To address this shortcoming it would be useful to establish a system at borders to ascertain whether a third country national is in possession of a valid residence card, residence permit or long-term visa, and if needed, to enable Member States to grant this person access to the Schengen area under the same conditions as an EU national (through the use of an eGate).A study should be conducted, to determine whether such a system could be established.

Beyond border management, there could be a third consideration for establishing a central information system on third-country nationals holding notably, a residence permit. Beneficiaries of European residence permits have to fulfil certain conditions. These may include limitations on the time they can spend outside the Member State that issued the permit, in order not to lose their right of residence and their access to certain social rights and services. Some Member States expressed a desire to also monitor travel movements of residence permit holders to assess compliance with these limitations.

Against this background the establishment of central repository of residence permits, residence cards and long-term visas issued by Member States, to store information on these documents (including on expiry dates and on their possible withdrawal) should be considered. The Commission should assess whether such a new EU tool is necessary, feasible and proportional to address the existing information gap regarding these categories of third-country nationals or whether other steps can be taken to serve the same purpose.

References to other actions in the Roadmap: Actions 41 and 42.
