



Council of the  
European Union

Brussels, 14 March 2019  
(OR. en)

7378/19

ENFOPOL 119  
JAI 278

**NOTE**

---

From: General Secretariat of the Council  
To: Law Enforcement Working Party

---

Subject: Work programme of Europol for 2019

---

Delegations will find attached the relevant section of the Europol Programming Document 2019-2021 which constitutes Europol's work programme for 2019.

**Europol Public Information**

---

**SECTION III - Work Programme 2019****1. Executive summary**

Europol's Work Programme 2019 gives a comprehensive overview of the regular work portfolio of the agency and at the same time describes the specific annual objectives for 2019 for the different areas of operation.

In 2019 Europol will continue providing the Member States with high quality operational support to investigations in the three key priority areas, aligned with the European Agenda on Security, namely serious and organised crime, cybercrime and counter-terrorism. While doing so the agency has to manage continuously growing data flows and demand for Europol's services, and keeping up with the pace of technological progress. In addition, Brexit and the future relationship between the United Kingdom and Europol will bring a unique set of challenges for the agency. While the solution will be agreed elsewhere the impact will need to be managed by Europol.

Next to Europol's usual tasks and responsibilities a number of developments will start or escalate in 2019 and those have been highlighted in the Work Programme. In summary the main initiatives foreseen are as listed below:

- In 2019 Europol will aim to achieve significant progress with the Integrated Data Management Concept (IDMC) and ensure the transition towards the novel information management architecture. In parallel and in order to prepare for the tasks assigned to Europol in the draft proposal for a Regulation establishing a framework for interoperability between EU information systems, a significant portion of Europol's work in the ICT domain is devoted to improving the efficiency of information sharing and the connectivity with relevant EU information systems and networks. Furthermore, by operating in an environment of dynamic technological progress, Europol makes the continuous effort to upgrade its ICT capabilities, systems and tools, to be able to respond to innovation adversely used for criminal purposes.
- Based on its newly acquired access to the Schengen Information System, Europol will set up a SIRENE office and develop relevant internal and external procedures for the information exchange and the processing of SIS II data for analytical purposes. Specific attention will be given also to the implementation of a sustainable solution for the FIU.net application, which should incorporate a proven anonymised/ pseudonymised cross-matching technique and ensure smooth processing of large volumes of data.
- The priorities of the EU Policy Cycle for organised and serious international crime 2018-2021 will remain again the main driver for the operational support provided by Europol to the MS' competent authorities in 2019. The agency will focus on the implementation of the tasks stipulated in the Operational Action Plans and will pay particular attention to setting-up the new priority areas such as criminal finances and money laundering and environmental crime. Furthermore, Europol will take additional initiative in the fight against drug trafficking following its Drug Strategy and against migrant smuggling organised networks in line with the objectives of the Malta Implementation Plan on migration.
- The renewed EU Cybersecurity Strategy and Directive on the combatting of fraud and counterfeiting of non-cash means of payment bring new assignments to the European Cybercrime Centre (EC3) and further boosts its current tasks. As mandated, EC3 is planning to expand its focus on cyber forensics and on monitoring and combating criminality on the Dark Web. Another major priority is to strengthen the capability for recovering encrypted criminal data and utilising the agency's potential to perform as a European centre of expertise on decryption. To this end Europol will be putting in place a decryption system in cooperation with the Joint Research Centre (JRC) which will lead to a significant increase in processing power.

29

### Europol Public Information

- In the area of counter-terrorism efforts to achieve greater information exchange among the relevant partners at EU level will continue, together with Europol's commitment to provide better and extended operational support to MS' investigations. A particular endeavour will target the expansion of the scope of the Cross Border Access to Electronic Evidence (SIRIUS) Project and the fulfilment of the actions to step up internet referrals and support to internet investigations by the EU IRU in the framework of the European Commission's Action plan to combat terrorism online.
- Specific attention will be paid in 2019 on how to improve the work on criminal analysis. At the EU level Europol will be contributing to the development of standard EU definitions and quality criteria for analysis products and training which should lead to improved cross-border collaboration and increased operational impact. In-house, the agency will be aiming to optimise processes and methodologies on how to deliver quality strategic analysis reports.
- 2019 will be the year for accelerating Europol's capabilities in the area of travel data processing and analysis following the new Travel Intelligence Roadmap of the agency. The new access to travel data is expected to enrich the intelligence picture in Europol's operational and strategic products. The support to the EU PIUs will be further developed, whereas the preparations for ETIAS will have started materialising. According to preliminary estimates, the volumes of data associated with these initiatives and Europol's role in the ETIAS will have significant implications on the agency's operational and ICT workload.
- In 2019 the ATLAS Network of Special Intervention Units will be affiliated within the structure of Europol. One main objective will be to establish links between ATLAS and Europol's CT and SOC communities, and facilitate the exchange of strategic and operational expertise and practices in accordance with the applicable rules.
- Last but not least, as a continuous endeavour the agency will keep investing in the optimisation of its corporate functions by focusing among others on establishing a new Europol Financial Regulation, adjusting HR policies according to the requirements of the TA 2(f) article of the Staff Regulation, improving the performance measurement and reporting, progressing with electronic management of documents and digitalisation of HR, financial and facilities processes. The implementation of the Strategic Housing Roadmap in 2019 which will comprise the relocation of a part of Europol's staff to a temporary satellite building together with the necessary expansion of ICT, security and administrative services will constitute another major effort for the year ahead.

Table: Overview of Objectives 2019  
Correlation between Strategic Objectives 2016-2020 and Objectives 2019

Strategic Objective 2016-2020	Europol WP Activity	Objective 2019
<b>Goal 1: Europol will be the EU criminal information hub, providing information sharing capabilities to law enforcement authorities in the MS</b>		
1.1. Develop the necessary ICT capabilities to maximise the exchange and availability of criminal information	A.1. Development of operational ICT capabilities	A.1.1. Advance the implementation of the new information management architecture and continue improving operational capabilities and tools by focusing on automation and modernisation.
		A.1.2. Advance interoperability and connectivity with information management systems at EU level to enhance information exchange.
1.2. Provide effective and immediate first-line information exchange	A.2. Information Hub	A.2.1. Broaden the information processing capabilities of Europol's Front Office.
		A.2.2. Utilise the newly acquired access of Europol to the Schengen Information System.

**Europol Public Information**

<b>Strategic Objective 2016-2020</b>	<b>Europol WP Activity</b>	<b>Objective 2019</b>
1.3. Strategically enhance partnerships with cooperation partners		A.2.3. Implement an effective cooperation process with external partners on the basis of Europol's External Strategy 2017-2020.
		A.2.4. Utilise new opportunities for cooperation with EU institutions and agencies.
<b>Goal 2: Europol will provide the most effective operational support and expertise to MS investigations by developing and employing a comprehensive portfolio of services</b>		
2.1. Support MS investigations in the area of Serious and Organised Crime (SOC)	A.3. Combating SOC	A.3.1. Improve procedures and operational approach to foster Europol's support to MS investigations against organised crime.
		A.3.2. Ensure the implementation of the objectives of the Malta Implementation Plan in the fight against organised crime related to migrant smuggling and THB.
		A.3.3. Undertake and support further improvements in the strategic and operational approach followed by the MS and Europol in targeting the reduction of drugs supply.
		A.3.4. Strengthen the fight against counterfeiting and intellectual property crime.
		A.3.5. Strengthen the fight against organised crime groups involved in fraud activities.
		A.3.6. Strengthen the fight against organised property crime.
2.2. Support MS investigations in the area of cybercrime	A.4. Combating cybercrime	A.4.1. Accelerate Europol's capabilities to provide support to MS' investigations in the area of cybercrime-related EU Policy Cycle priorities 2018-2021.
		A.4.2. Further develop Europol's capability for recovering encrypted criminal data and utilise the agency's potential to perform as a European centre of expertise on decryption.
		A.4.3. Foster international cooperation and identify joint activities to address common challenges in the cybercrime and cyber-enabled crime area in a unified manner.
2.3. Enhance cooperation in the area of counter-terrorism (CT)	A.5. Counter-terrorism	A.5.1. Promote and facilitate greater information exchange in the area of counter-terrorism and provide better and extended operational support to Member States' investigations.
		A.5.2. Expand the scope of the Cross Border Access to Electronic Evidence (SIRIUS) Project.
		A.5.3. Enhance Europol's internet referral capabilities for prevention and investigation in the context of the EU Internet Forum Action Plan to Combat Terrorist Online Content.
		A.5.4. Implement the affiliation of the ATLAS Network of Special Intervention Units within the structure of Europol.
2.4. Develop and manage high quality	A.6. Provision of cross-	A.6.1. Contribute to the development of a common EU view on criminal analysis.

**Europol Public Information**

<b>Strategic Objective 2016-2020</b>	<b>Europol WP Activity</b>	<b>Objective 2019</b>
analytical support and an evolving portfolio of cross-cutting operational capabilities	cutting operational capabilities	A.6.2. Strengthen Europol's capabilities to deliver quality strategic reports.
		A.6.3. Develop Europol's capabilities in the area of travel intelligence in line with the Travel intelligence Roadmap.
		A.6.4. Reinforce the provision of horizontal support to investigations by advancing the development of specialist law enforcement techniques.
		A.6.5. Increase the provision of comprehensive financial intelligence to MS regarding money laundering, asset recovery, corruption and terrorism financing, including possible links to other criminal areas.
<b>Goal 3: Europol will be an efficient organisation with effective governance arrangements and a positive reputation</b>		
3.1. Ensure effective, efficient and accountable management of Europol's resources	A.7. Governance, support and administration	A.7.1. Continue optimising Europol's corporate functions.
		A.7.2. Progress towards the rationalisation and expansion of Europol's capabilities in order to accommodate the growth of the agency.
3.2. Promote the added value and achievements of EU law enforcement cooperation to stakeholders and EU citizens		A.7.3. Establish a new strategy for effective awareness raising on Europol's products and services to law enforcement stakeholders.

## 2. Activities

### A.1. Development of operational ICT capabilities

#### Overview

Ensuring that the optimum communication and operational solutions are in place for operational information exchange, data cross-checking, knowledge sharing and analysis is one of the core elements of Europol's mandate. The agency makes the continuous effort to evolve its ICT capabilities, systems and tools, or deliver new advanced ones, to support its function as the European criminal information hub and as a provider of operational support for MS investigations.

Law enforcement operates in an environment of dynamic technological progress and innovation adversely used for criminal purposes. In this context, the agency faces the challenge of continuously increasing information flow and complexity of data sets which requires permanent endeavour and ultimately fundamental changes in the management of information.

Based on the Europol Regulation the agency works towards the re-designing of its information management architecture which aims at streamlining and modernising the execution and increasing the effectiveness of data processing for the benefit of all partners involved. To that effect, Europol has set up a multi-year transformation programme, New Environment for Operations (NEO) that leverages the possibilities of the Regulation and implements the concept of Integrated Data Management.

The NEO roadmap will see a significant acceleration in the transition towards a capability-based approach on ICT's application landscape, ensuring the advanced and mature application of the Integrated Data Management at Europol.

With respect to the latter Europol is preparing to follow up on the tasks assigned to it in the draft proposal for a Regulation establishing a framework for interoperability between EU information systems<sup>9</sup>.

The replacement of existing operational ICT solutions with capabilities bringing forward innovative and novel techniques, like artificial intelligence, machine learning, advanced analytics will enable the EU Law Enforcement community to cooperate better, easier and more efficiently. In the meantime existing systems will remain fully supported until their functions can be accommodated by NEO; where necessary, bridging solutions will be put in place.

Key capabilities that have been identified for 2019 are:

- Analysis capability
- Messaging Capability (incl. SIENA)
- Data Sharing capability (incl. EIS)
- Data Management capability
- SMART capability
- Forensic capability
- Operations support capability
- Technical infrastructure capability

The implementation of the IDMC will duly incorporate data protection safeguards as prescribed in Europol's Regulation. Any work on interoperability and connectivity with

<sup>9</sup> COM(2017) 794 final

## Europol Public Information

information management systems at EU level will build on the provisions for protection of fundamental rights and freedoms of natural persons in the legal instruments of the respective systems and other relevant EU law (e.g. on data protection, privacy, non-discrimination, etc).

### Recurrent actions

<b>Core operational ICT capabilities, specialised systems and tools and key IM initiatives</b>
<p>Development, implementation and/or maintenance of capabilities<sup>10</sup>:</p> <ul style="list-style-type: none"><li>○ Messaging Capability incl. Secure Information Exchange Network Application (SIENA); Universal Message Format (UMF);</li><li>○ Data Sharing Capability incl. Europol Information System (EIS) with (semi)automated functionalities to input data (Data Loaders) and to search data (QUEST - Querying Europol Systems); Internet Referral Management Application (IRMA), including specialised internet scanning tools; FIU.net; Automation of Data Exchange Process (ADEP);</li><li>○ Data Acquisition Capability incl. Large File Exchange (LFE); Decryption Platform;</li><li>○ Data Management Capability incl. Unified Search Engine (USE); Unified Audit System (UAS) for data protection;</li><li>○ Analysis Capability incl. Europol Analysis System (EAS);</li><li>○ SMART Capability incl. Automated Biometrics Identification System (ABIS); Face Recognition system (FACE); Enhanced Risk Entities Solution (ERES) and machine learning;</li><li>○ Knowledge Sharing Capability incl. Europol Platform for Experts (EPE);</li><li>○ Forensics Capability incl. Image and Video Analysis Solution (IVAS); Europol Malware Analysis Solution (EMAS); EC3 Service Design and forensic tools (e.g. Mobile Forensic Kit);</li><li>○ Technical Infrastructure Capability incl. Identity and Access Management (IAM);</li><li>○ Operations Support Capability incl. European Tracking Solution (ETS); Mobile Office.</li></ul> <p>Connectivity and support to:</p> <ul style="list-style-type: none"><li>○ Schengen Information System (SIS II)</li><li>○ Visa Information System (VIS)</li><li>○ Eurodac</li><li>○ Passenger Name Records (PNR) network</li><li>○ Prüm framework</li></ul>
<b>Main tasks</b>
<p><i>Business product management of Information Management systems</i></p> <ul style="list-style-type: none"><li>○ Represent and advocate for end users' interests;</li><li>○ Manage the product lifecycle from concept to phasing out;</li><li>○ Perform business analysis;</li><li>○ Identify new opportunities, product enhancements and extensions;</li><li>○ Identify, specify and prioritise features, functionality and capabilities;</li><li>○ Act as a Senior User in ICT projects;</li><li>○ Facilitate the design, development and launch of new versions of the product;</li><li>○ Promote product awareness and deliver training;</li><li>○ Support end users, including the facilitation of issue resolution;</li><li>○ Carry out standard configuration changes;</li><li>○ Report on product usage;</li><li>○ Develop, maintain and execute product roadmap;</li><li>○ Develop expertise and keep up to date with technological advances;</li></ul>

<sup>10</sup> The list represents an initial mapping of operational ICT capabilities and the corresponding solutions.

**Europol Public Information**

<ul style="list-style-type: none"> <li>○ Facilitate the development and implementation of high impact and differentiated product positioning;</li> <li>○ Manage business cases for establishing access to relevant EU information systems;</li> <li>○ Contribute to the work on interoperability and connectivity of IM systems at EU level;</li> <li>○ Represent Europol in relevant committees and boards, e.g. SIS II, VIS, EURODAC, EES, UMF, DAPIX and ADEP.</li> </ul>
<p><i>Embedded ICT Security</i></p> <ul style="list-style-type: none"> <li>○ Define and monitor security standards;</li> <li>○ Check ICT infrastructure for weaknesses;</li> <li>○ Design and build ICT security improvements;</li> <li>○ Handle security-related calls;</li> <li>○ Enable and enforce secure software coding best practices in software development;</li> <li>○ Review solutions, spot security issues and propose improvements;</li> <li>○ Define and implement security processes and procedures, including staff training;</li> <li>○ Perform audits on implementation of the security processes and procedures;</li> <li>○ Define roadmap and necessary steps to ensure ICT continuity.</li> </ul>
<p><i>Solutions Operations</i></p> <ul style="list-style-type: none"> <li>○ Daily / periodic maintenance of the solutions and infrastructure;</li> <li>○ Own and evolve monitoring &amp; response operations practices;</li> <li>○ Create and periodically test backups;</li> <li>○ Maintain the Configuration Management Database for all non-work place services related systems and components;</li> <li>○ Patch periodically all network, server, storage, middleware and application components;</li> <li>○ Implement technical product manager roles for all commercial off-the-shelf solutions.</li> </ul>
<p><i>Solutions Deployment</i></p> <ul style="list-style-type: none"> <li>○ Define and manage the Change and Release management processes;</li> <li>○ Implement all changes into all environments of the Europol ICT landscape;</li> <li>○ Develop and maintain processes and tooling for automated deployments;</li> <li>○ Provide tools to be used during the software development cycle;</li> <li>○ Own the Team Foundation Server system (or equivalent) for deployment in Production, Staging and Test.</li> </ul>
<p><i>Law Enforcement Accelerated Provisioning</i></p> <ul style="list-style-type: none"> <li>○ Coordinate the provisioning of ad-hoc capabilities to support LE operational needs;</li> <li>○ Engineer and deploy ad-hoc processing environments;</li> <li>○ Engineer and implement data pre-processing tools;</li> <li>○ Identify opportunities for reuse, and define new services when appropriate;</li> <li>○ Guarantee security and data protection considerations.</li> </ul>
<p><i>Application Delivery Services</i></p> <ul style="list-style-type: none"> <li>○ Provide application development services across multiple delivery models (e.g. external software factory);</li> <li>○ Ensure consistent software engineering practice (including secure coding);</li> <li>○ Define delivery methods, tools and standards.</li> </ul>
<p><i>Test &amp; Quality Assurance</i></p> <ul style="list-style-type: none"> <li>○ Own the quality assurance processes and standards;</li> <li>○ Perform functionality, continuity and security testing related to software solutions and infrastructure changes;</li> <li>○ Continuously develop an automated testing approach.</li> </ul>
<p><i>ICT Solution Architecture &amp; Engineering Coordination</i></p> <ul style="list-style-type: none"> <li>○ Own the overall Solution Portfolio;</li> <li>○ Ensure that ICT solutions are aligned with the intended capability portfolio;</li> <li>○ Own the end-to-end design of individual solutions;</li> </ul>



### Europol Public Information

<ul style="list-style-type: none"> <li>○ Provide services to implementation projects;</li> <li>○ Create enabling technology roadmaps, including replacement of obsolete solutions;</li> <li>○ Proactively identify and propose technology-driven innovation opportunities.</li> </ul>
<p><i>Portfolio and Project management</i></p> <ul style="list-style-type: none"> <li>○ Create ICT Workplan and monitor its execution;</li> <li>○ Ensure that the projects and work packages deliver according to agreed schedule, scope and cost;</li> <li>○ Proactively identify and manage risks, perform stakeholder management and relevant communication to involved parties;</li> <li>○ Support key projects with technical expertise;</li> <li>○ Coordinate ICT work planning capacity; validate estimations and assumptions.</li> </ul>
<p><i>ICT Capabilities Innovation</i></p> <ul style="list-style-type: none"> <li>○ Maintain the portfolio of ICT capabilities and business solutions, and their respective roadmaps, while ensuring evolution in alignment with business needs and strategy;</li> <li>○ Analyse business capabilities and needs, propose opportunities for ICT innovation, and drive architectural decisions;</li> <li>○ Establish requirements for ICT solutions aligned to business needs and the Business and Information Architecture;</li> <li>○ Analyse processes and user interaction to support development and procurement initiatives with the appropriate set of solution requirements;</li> <li>○ Propose functional design to reach the optimal implementation considering business needs and technical capabilities.</li> </ul>

### 2019 Objectives

A.1.1. Advance the implementation of the new information management architecture and continue improving operational capabilities and tools by focusing on automation and modernisation.\*

#### Actions

#### Data Management Capability

Complete the first phase of the central data repository (data lake). Improve and extend the means for data intake as part of the data management capability.

Set up information processing for multiple purposes (search and cross-check, strategic/thematic analysis and operational analysis).

Continue expanding the access to selected information systems from multi-security level infrastructure (e.g. for EIS and QUEST) including changes in the applications and the infrastructure.

Increase the use of structured data by Europol and further facilitate the provision of structured data by MS using UMF. Continue supporting improvement of UMF standards.

#### Analysis Capability

Start implementing the Analysis Capability, based on the overarching NEO design that will be completed by the end of 2018. The Analysis Capability will include -among other elements- the future of the current Europol Analysis System.

#### Messaging Capability

Further support the roll-out of SIENA to more competent authorities and law enforcement communities as part of the

## Europol Public Information

---

messaging capability implementation. Continue improving SIENA usability, the access from BPL networks and the provision of statistics/business intelligence. Advance with enabling usage of the messaging capability for users of other Europol capabilities and systems such as the analytical system, LFE, EMAS and EU IRU.

Analyse the impact of Brexit once the final agreement is known and start implementing the required changes in identified solutions.

### **Data Sharing Capability**

Design and start implementing the Data Sharing capability, including the future shape of the current EIS taking into account a way forward on the dataloader schema, ensuring compatibility with UMF and integration with Europol's capability landscape. As a bridging solution, maintain and improve the current EIS, in particular by dismantling the current transfer of ownership process from person object Cross-border crime checks.

Expand the search self-service functionality by more advanced search mechanisms, offering immediate insight in validated entities and links between them, as available in the wider Europol data set, governed by appropriate user access privileges. These services will be offered as independent tools, and, as a bridging solution, be incorporated into EIS.

Explore the possibility to extend the capacity for the direct loading of data into EIS by third parties.

Continue automating the immediate follow-up processes through SIENA for successful (self-)searches on Europol's and Member States' data. Depending on the specific approach to be chosen by MS this initiative may trigger changes to systems and underlying architecture to meet availability targets and processing volumes.

Expand QUEST functionality to include the search self-service functionality described above. Grant several pilot Member States access to Europol's Analysis Projects through the QUEST web service on a hit/no hit basis. Extend QUEST with searches for new object types (e.g. ID documents, means of transportation, means of communication and offences). Implement a fuzzy search mechanism on persons in QUEST. Update QUEST to use UMF2.0. Extend the EIS statistical tool to include also statistical data on QUEST.

Significantly increase QUEST performance to cope with its wide roll out to the front-line law enforcement officers and its use for automated, system-to-system search and cross-checking.

In order not to create bottle necks in other areas also performance enhancements will be implemented in EIS and dataloaders (effective and efficient data insertion and management) as well as in SIENA (effective and efficient communication and follow-up). All improvements will take into account UMF as the default, cross-border data exchange standard.

Roll-out Internet Referral Management application (IRMA) to Member States and rebuild Check-the-Web functionality in IRMA.

---

**Analytics and Reporting implementation**

Complete the design of the Corporate Reporting taking into account the new data repository and start implementing the Analytics and Reporting capability.

**Forensics Capability**

In line with IDMC, start implementing the merge of the Computer Forensics Network (CFN) into the Operational Network, in order to maximise the value of available data (currently in separate networks) and consolidate toolsets.

**SMART Capability**

Continue introducing smart innovative capabilities that are crucial for automating and pseudonymising cross-checking, pattern search, effective processing of large and diverse data volumes. Step up the creation of the Data Science capability in ICT to support techniques such as Image and video analysis, speech processing, Natural Language Processing, Biometrics, Sensor generated data, etc.).

**Technical Infrastructure**

Harmonise further the IAM landscape of Europol by integrating more systems with IAM and taking further steps towards establishing single enterprise identity taking into account different networks and security standards, including IAM for BPL business solutions, flexibility in IAM workflows and improved reporting capabilities for enhanced IAM governance.

Fine-tune the EPE upgrade and ensure a smooth transition to the new version. Upgrade the EPE on the Operational Network. Improve the authentication process to ensure higher security.

**Operations Support Capability**

Explore the need and possibilities for setting up an operational collaboration environment for conducting joint analysis of a strategic or thematic nature among trusted expert communities.

---

Expected results

State of the art forms of data management and processing are in place resulting in process optimisation and resource efficiency, and enhanced information security, user experience, decision-making and identification of links.

The MS' needs in terms of operational support are better met through the evolution of communication and operational tools and facilities.

A.1.2. Advance interoperability and connectivity with information management systems at EU level to enhance information exchange.

Actions

With the support of eu-LISA build new Europol connection to Schengen Information System (SIS II) which should allow for the utilisation of all access rights to the system (including biometrics). Enable additional batch searches (e.g. ID documents).

Meet the technical requirements for setting up a SIRENE office within Europol having direct access to the SIRENE network.

---

**Europol Public Information**

Establish Europol’s access to Visa Information System (VIS) with the support of eu-Lisa.

Analyse the requirements for establishing a new Europol access to Eurodac based on the recast of Eurodac regulation.

Undertake detailed analysis on the technical requirements and possible solutions for Europol to fulfil its specific tasks in reference to EU Travel Information and Authorisation System (ETIAS).

Undertake detailed analysis of the technical requirements and the resources required for the implementation of Europol’s access to Entry-Exit System (EES).

Depending on MS interest and involvement, as well as the financial implications for Europol, continue supporting the ADEP network as the central coordinating body and undertake follow-up actions based on the assessment of the testing results of the EPRIS-ADEP pilot project in 2018.

Finalise the analysis on the possibility for Europol to become an information exchange partner in the Prüm framework, in particular regarding the legal constraints and the technical and financial requirements. Come up with the solution design, if the conclusions of the analysis proved favourable.

Provide technical advice on initiatives related to the implementation of the EU Roadmap on information exchange and interoperability. Follow-up on the recommendations relevant for Europol of the High Level Expert Group on Interoperability and the draft proposal for a Regulation establishing a framework for interoperability between EU information systems, e.g. on the European Search Portal, Shared Biometric Matching Service, SISII Hit Repository etc.

Expected results

The MS’ needs in terms of efficient access to information are better met.

Interoperability and complementarity of Europol’s data management landscape and specific tools with other EU information management systems leads to increased and more efficient exchange of information.

*(\* The level of implementation of objectives or actions marked with an asterisk throughout the Work Programme depends on the availability of additional resources.)*

Indicators <sup>11</sup>	Latest result Q3 2018	Target 2019
<i>Operational Stability - Uptime of Core Systems</i>	99.6%	98%
<i>Core business project and workpackages delivery (% of milestone points achieved)</i>	-	75%
Number of organisational sub entities’ SIENA mailboxes in MS and TP connected to SIENA	1,414	1,800

<sup>11</sup> Indicators marked in italics are the Corporate Key Performance Indicators.

### Europol Public Information

Indicators <sup>11</sup>	Latest result Q3 2018	Target 2019
<i>Number of SIENA messages exchanged</i>	813,306	1,190,000
<i>Number of SIENA cases initiated</i>	56,231	88,000
<i>% of all SIENA messages received by Europol containing structured data</i>	13%	15%
<i>Number of objects in the EIS (MS+Europol)</i>	1,217,667	1,500,000
Number of person objects in the EIS	196,576	240,000
<i>Number of EIS searches</i>	2,652,811	3,500,000
Number of MS EIS data loaders	11	17
Cross-border crime checks (CBCC) related to persons	2,251	2,000
Number of active expert platforms on the EPE	51	52
Number of EPE user accounts	12,922	15,000
% of active users on the EPE	47%	45%
Number of MS connected to QUEST production	1	6

## A.2. Information Hub

### Overview

Europol aims to be the EU criminal information hub, providing information-sharing capabilities to law enforcement authorities in the Member States. In this context, Europol's Front Office is the gateway for all operational information and intelligence channelled through Europol and strives to deliver fast, real-time and quality services to its stakeholders. Another important element of being the EU criminal information hub is the strategic enhancement of relationships with cooperation partners, to ensure that necessary strategic and operational information is made available and exchanged through Europol to better support the MS in tackling serious and organised crime, cybercrime and terrorism.

Europol's Front Office is responsible for the handling of all incoming information and for managing the workflow of non-prioritised cases in terms of data processing, data handling and hit reporting. It also provides support to specific operations and action days both from the office and on the spot. In case of serious incidents it initiates emergency procedures and coordinates Europol's immediate response. Finally, the Front Office presents up-to-date business intelligence to management, enabling decision making on a permanent 24/7 basis and assures the continuity of the operational business outside office hours.

Facilitating the cooperation among all competent law enforcement authorities including Customs and Counter-Terrorism services in the Member States is a crucial element of Europol's work and mandate. The agency supports the Liaison Bureaux of Member States and other cooperation partners at Europol and maintains Europol liaison offices in other countries and organisations. It organises on a regular basis consultations with the Heads of the National Units of MS.

In view of the global challenges which the EU is facing, effective investigations depend often on the information exchange with third countries and private partners. In the past years Europol succeeded in establishing cooperation with key external partners and it will continue working on the implementation of the different cooperation agreements as well as on increasing outreach to other countries following the requirements of the new Europol regulation.

At the same time, Europol aims to further strengthen its partnership with Interpol and relevant EU agencies and institutions, in particular those active in the area of Justice and Home affairs in order to ensure complementarity and maximum benefit from possible synergies.

### Recurrent actions

#### Front Office

##### *Operational Information Management*

- Monitor operational data on 24/7 basis as the single point of entry for any incoming information from stakeholders;
- Decide on the acceptance of information into Europol's databases;
- Assign (distribute) operational messages within the Operations Directorate;
- Process and handle non-priority cases and manage related information hits including evaluation and reporting (cross-matching);
- Process and handle urgent messages in priority cases, in close cooperation with competent analysis projects;
- Process biometric data;

**Europol Public Information**

<ul style="list-style-type: none"> <li>○ Provide permanent monitoring and reporting of Open Source information;</li> <li>○ Manage EIS operational data including the insertion of data on behalf of third parties and hit management;</li> <li>○ Manage operational information exchange with third parties.</li> </ul>
<p><i>Support of Operations</i></p> <ul style="list-style-type: none"> <li>○ Act as 24/7 contact point for urgent operational requests from MS Liaison bureaux/Europol's National Units/competent authorities and for officers' reporting during on-the-spot deployment;</li> <li>○ Maintain organisational overview of on-the-spot deployments;</li> <li>○ In close cooperation with the Special Tactics team and other departments, guarantee 24/7 access to expertise and specialised operational knowledge;</li> <li>○ Manage the overview of mobile offices and other operational equipment;</li> <li>○ Manage the operational rooms;</li> <li>○ Support the coordination of operations and large-scale joint actions; Organise and chair corresponding planning meetings;</li> <li>○ Provide remote support to on-going actions/operations/major international events/on-the-spot deployments.</li> </ul>
<p><i>Initiating immediate actions and crisis response mechanisms</i></p> <ul style="list-style-type: none"> <li>○ Initiate the emergency procedures and crisis response steps in case of operational emergencies / terrorist attacks within the EU or impacting the security of the EU;</li> <li>○ Provide support to crisis management during serious incidents;</li> <li>○ Coordinate Europol's immediate response together with other relevant units and stakeholders;</li> <li>○ Initiate specialised assistance;</li> <li>○ Liaise with Europol's partners (MS and third parties) affected/involved.</li> </ul>
<p><i>Business Intelligence</i></p> <ul style="list-style-type: none"> <li>○ Prepare weekly intelligence briefing reports to inform internally about main operations, trends and patterns;</li> <li>○ Maintain dashboards for management to provide business information for decisions;</li> <li>○ Monitor on 24/7 basis information flow, requests for operational support and open sources to enable fast information to management when necessary;</li> <li>○ Further develop, maintain and deliver the 3-month induction training for newly recruited analysts; Contribute to the delivery of the EIS and SIENA trainings;</li> <li>○ Host visits to the Front Office operational rooms.</li> </ul>
<p><b>Strategic cooperation</b></p>
<p><i>Strategic cooperation with MS</i></p> <ul style="list-style-type: none"> <li>○ Manage strategic cooperation of Europol with MS;</li> <li>○ Coordinate Europol participation in the Management Board (MB);</li> <li>○ Coordinate and prepare meetings of the Heads of Europol National Units (HENUs);</li> <li>○ Organise study weeks for staff from Europol National Units;</li> <li>○ Support the liaison officers' community based at Europol, including by facilitating regular Heads of LB and Heads of Desk meetings;</li> <li>○ Support the Joint Investigation Teams (JIT) including the provision of funding in cooperation with Eurojust.</li> </ul>
<p><i>Strategic cooperation with third countries</i></p> <ul style="list-style-type: none"> <li>○ Manage strategic cooperation of Europol with third countries;</li> <li>○ Support the implementation of the operational agreements with Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, Former Yugoslav Republic of Macedonia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland and Ukraine, and the working arrangement with Israel;</li> <li>○ Support the implementation of the operational agreement with the USA and manage the Liaison Office in Washington;</li> </ul>

### Europol Public Information

<ul style="list-style-type: none"> <li>○ Support the implementation of the strategic agreements with China, Russia, Turkey and United Arab Emirates. The strategic agreement with Brazil is pending entry into force;</li> <li>○ Manage the deployments of Europol's Liaison officers to the Western Balkans;</li> <li>○ Monitor the implementation of agreements and the fulfilment of obligations and commitments.</li> </ul>
<p><i>Strategic cooperation with EU institutions, agencies or bodies</i></p> <ul style="list-style-type: none"> <li>○ Manage strategic cooperation of Europol with EU institutions, agencies or bodies; manage the Liaison Office in Brussels;</li> <li>○ Provide (technical) advice and contribute to the implementation of new EU political and legislative initiatives;</li> <li>○ Support the implementation of the operational agreements with Eurojust and Frontex;</li> <li>○ Support the implementation of the strategic agreements with CEPOL, ECB, ECDC, EEAS, EMCDDA, ENISA, EUIPO, EU-LISA, the European Commission and OLAF;</li> <li>○ Collaborate with other relevant EU agencies such as EASO, EMSA and FRA, and contribute to the work of the JHA Agencies Network.</li> </ul>
<p><i>Strategic cooperation with international and regional organisations</i></p> <ul style="list-style-type: none"> <li>○ Manage strategic cooperation of Europol with international organisations;</li> <li>○ Support the implementation of the operational agreement with Interpol and manage Europol's Liaison Offices in France and Singapore;</li> <li>○ Support the implementation of the strategic agreements with UNODC and WCO;</li> <li>○ Support the work of regional organisations and collaboration platforms such as the Baltic Sea Task Force, Danube River Strategy group, Western Balkan regional initiatives, the Eastern Partnership, MAOC-N, Afripol, the Western Africa Platforms, Aseanapol and Ameripol.</li> </ul>
<p><i>Legal services - EU and International Law</i></p> <ul style="list-style-type: none"> <li>○ Provide legal advice on the implementation of Europol's legal framework and data protection rules;</li> <li>○ Advice on legality and compatibility of new Europol initiatives with EU law, as well as on new EU initiatives having an impact on Europol;</li> <li>○ Implement the external relations regime as per the Europol Regulation;</li> <li>○ Conclude Administrative and Working Arrangements;</li> <li>○ Upon request provide assistance to the Commission's negotiations of international agreements and / or input to the process of preparing adequacy decisions;</li> <li>○ Provide legal advice on new possibilities for case by case cooperation with any third country, in the absence of an agreement or adequacy decision;</li> <li>○ Conclude undertakings from third countries, international organisations and EU bodies exchanging personal data with Europol;</li> <li>○ Implement and guide on new possibilities for cooperation with private parties stemming from the new Europol Regulation.</li> </ul>

### 2019 Objectives

A.2.1. Broaden the information processing capabilities of Europol's Front Office.	
Actions	<p>Increase the capability of the Front Office to extract the relevant operational data from incoming structured and unstructured information by using automations and utilising machine learning capabilities.</p> <p>Maintain the Front Office capacity to respond to MS requests in an expeditious way.*</p> <p>Ensure the efficient management, including the application of clear prioritisation criteria, of an extensive fleet of Mobile</p>



## Europol Public Information

---

	<p>Offices in response to the growing demand for on-the-spot support and the increasing number of operational missions in line with the Malta declaration.</p> <p>Further facilitate the coordination among stakeholders during the Joint Action Days. Ensure the use of communication channels as predefined in the operational action plan of the respective JAD and promote the use of templates/agreed documents to facilitate a more effective information exchange.</p> <p>Provide support to major international events. In particular carry on the engagement with the expert group on the implementation of the UEFA 2020 coordination centre, including the preparation of the final action plan for the set-up</p> <p>Accommodate the potentially significant task of facilitating the exchange of information between EU MS and UK post-Brexit.</p>
Expected results	<p>More efficient data processing is in place leading to optimisation of analytical work.</p> <p>Increased quality and completeness of Europol's intelligence picture allows for more effective response to MS operational cases and crisis situations.</p>

---

### A.2.2. Utilise the newly acquired access of Europol to the Schengen Information System.

Actions	<p>Set up a SIRENE office<sup>12</sup> within Europol and develop relevant internal and external procedures for the information exchange and the processing of SIS II data for analytical purposes.</p> <p>Provide training on the SIS II and the newly acquired possibilities for Europol to all relevant Europol staff involved in data processing and analysis.</p> <p>Organise an event with the Heads of SIRENE Bureaux with special focus on enhancing cooperation and addressing the practical challenges of the implementation of the new legislation and the Council Conclusions.</p> <p>Stimulate the discussion on Europol's role in SIS II with a view to assessing and utilising opportunities for evolving the SIRENE office into a fully-fledged 'EU SIRENE Bureau' having the possibility to insert in SISII high-profile individuals or important objects on behalf of Third Parties.</p>
Expected results	<p>Increased quality and completeness of Europol's intelligence picture with regards to SIS II alerts and through the exchange of supplementary information.</p>

---

### A.2.3. Implement an effective cooperation process with external partners on the basis of Europol's External Strategy 2017-2020.

Actions	<p>Maintain effective operational cooperation with the UK from the point the country ceases to be a Member State of the EU<sup>13</sup>.</p>
---------	--

---

<sup>12</sup> Europol's SIRENE Office will have limited functions compared to the MS' SIRENE Bureaux. While it will have access to SIS alerts and the exchange of supplementary information, it will not have the mandate to insert alerts into the SIS II system.

<sup>13</sup> In compliance with the EU-UK Withdrawal Agreement (provided it enters into force).

## Europol Public Information

Improve the framework for cooperation with MENA countries, e.g. by concluding working and potentially administrative arrangements to implement international agreements allowing for the exchange of personal data (as necessary), to allow for effective cooperation with these countries especially in the area of terrorism, migrant smuggling and THB. Make use of available EU resources and representations in third countries.

Assist the European Commission, where requested, in the negotiation of operational agreements according to Art.218 TFEU with MENA countries and the review of existing agreements according to Art.25(4) of Europol's Regulation.

Establish or reinforce cooperation with other selected high-priority third countries and partners as listed in the Management Board decision on Europol's external relations priorities in line with operational needs and as concluded in the mid-term review of the implementation of Europol's External Strategy 2017-2020.

Utilise the deployments of Europol Liaison officers to the Western Balkan countries to establish closer cooperation and encourage increased information exchange and joint investigations on serious and organised crime, counter-terrorism and migrant smuggling criminal networks. Prepare a plan for delivering an evaluation of the deployments in 2020.

---

Expected results	Increased involvement of Europol in information exchange with third countries and better access to information from abroad.  Improved cooperation and joint undertakings with third countries and organisations leading to an increased operational impact.
------------------	---

### A.2.4. Utilise new opportunities for cooperation with EU institutions and agencies.

Actions	Engage in a joint strategic reflection on the future of the EU security infrastructure and the role of the JHA agencies, as part of Europol's chairmanship of the Justice and Home Affairs Agencies Network (JHAA network).  Conclude the working arrangement with OLAF and implement the indirect access by OLAF, on the basis of a hit-no hit system, to information held by Europol.*  With the support of Eurojust initiate any preparatory work required for establishing a working arrangement with the upcoming European Public Prosecutor's Office (EPPO).  Increase coordination between Europol Analysis Projects and Eurojust Contact Points. Provide Eurojust access to Europol data on a hit-no hit basis.*  Invest further efforts in establishing working or administrative arrangements with the partner organisations required for achieving full operational capacity of the Information Clearing House.  Reinforce efforts to set up cooperation with EEAS and the EU Delegations, in order to improve the direct links to Europol's work and to progress on embedding the law enforcement component into CSDP missions.
---------	---

---

**Europol Public Information**

	<p>Ensure reinforced cooperation with eu-Lisa and Frontex with regard to the implementation of legislative files such as SIS II, ETIAS, interoperability of the EU information management systems, etc.</p> <p>Explore possible arrangements for deploying a Europol liaison officer to Frontex for coordination of implementation plans, alignment of operational activities and information exchange in the area of migrant smuggling.</p> <p>Exploit potential areas for collaboration stemming from the establishment of the European Union Agency for Asylum (ex. EASO).</p> <p>Review the performance of the Brussels office in terms of efficiency.</p>
Expected results	Alignment of actions among EU agencies leading to better operational results.

(\* The level of implementation of actions marked with an asterisk throughout the Work Programme depends on the availability of additional resources.)

Indicators	Latest result Q3 2018	Target 2019
<i>Speed of first-line response to MS requests (days)</i>	7.2	7
<i>Accepted contributions to be processed</i>	55,131	75,000
<i>Operational Information Backlog (number of operational contributions pending processing)</i>	2,702	1,500
<i>% of total SIENA messages exchanged (by Europol) outside of office hours</i>	9%	10%
<i>Hit rate (Number of cross match reports and SIENA hit notifications per 100 accepted contributions)</i>	9.2%	9%
<i>Number of Mobile office deployments</i>	306	400
<i>SIENA messages exchanged by third parties (TP)</i>	116,267	222,000
<i>Operations supported by Europol involving cooperation partners</i>	569	780
<i>Operations supported by Europol involving private partners</i>	57	72

### A.3. Combating Serious and Organised Crime

#### Overview

The work of Europol in the fight against serious and organised crime is delivered through its European Serious and Organised Crime Centre (ESOCC). The centre aims at providing the most effective operational support to prioritised cases and this encompasses criminal intelligence analysis, on-the-spot and real time information exchange and expertise, and operational capabilities support to Member States.

Europol has embedded the principles of intelligence-led policing in its structure, processes and resources. The agency facilitated the implementation of the first two EU Policy Cycles for organised and serious international crime and is currently working on the next one covering the period 2018-2021 which will be again the main driver for the operational support provided by Europol to MS competent authorities in 2019.

ESOCC's work focuses on Organised Crime Groups (OCGs) active in the areas of Commodities, Economic and Property Crimes. Within each group the Analysis Projects (APs) are clustered and aligned to the priorities of the EU Policy Cycle. APs are focused on processing data, drafting analysis and knowledge reports, organising operational meetings and providing expertise and on-the-spot support to MS investigations, including Joint Action Days.

ESOCC also includes the European Migrant Smuggling Centre (EMSC) which encompasses Europol's work on criminal activities related to irregular migration. The goal of the EMSC is to have a decisive role in proactively supporting MS to target and dismantle organised crime networks involved in migrant smuggling, with special attention provided to existing and emerging EU hotspots. From 2017, particular focus has been placed on the Central Mediterranean area in line with the Implementation Plan stemming from the Malta Declaration on migration. A closely linked dedicated analysis project on Trafficking in Human Beings deals with different forms of human exploitation.

#### Recurrent actions

Main tasks
<p><i>Provision of Operational Support</i></p> <ul style="list-style-type: none"> <li>○ Handle ESOCC information; monitor information flows;</li> <li>○ Coordinate and support ESOCC operations;</li> <li>○ Perform ESOCC intelligence analysis and provide analytical support;</li> <li>○ Support MS in identifying High Value Targets (HVT) - individuals and criminal organisations constituting the highest risk of organised and serious crime; establish Operational Task Forces on particular HVT;</li> <li>○ Support MS with operational capabilities and expertise that are not available widely at national level to enhance cost-effectiveness;</li> <li>○ Work closely with front-line investigators by providing on-the-spot, real-time information exchange and expertise (Mobile Forensic Kit, Mobile Office);</li> <li>○ Manage migrant smuggling-related operational information received from the guest officers deployed at the hotspots;</li> <li>○ Support MS by using the most suitable, tailor-made operational delivery models, including short and longer-term deployments of Europol experts (e.g. regarding technical support for counterfeit goods and currency, dismantling of drug labs);</li> <li>○ Provide testimony in court;</li> </ul>

**Europol Public Information**

<ul style="list-style-type: none"> <li>○ Set up operational meetings and support Joint (EMPACT) Action Days.</li> </ul>
<p><i>Implementation of EU Policy Cycle priorities</i></p> <ul style="list-style-type: none"> <li>○ Support the EU Policy Cycle and increase its impact on the set priorities;</li> <li>○ Support the implementation of Multi-Annual Strategic Plans (MASP);</li> <li>○ Support the implementation of Operational Action Plans (OAP) to combat priority threats.</li> </ul>
<p><i>Strategy and Outreach</i></p> <ul style="list-style-type: none"> <li>○ Coordinate strategic intelligence collection and management;</li> <li>○ Provide dedicated strategic and tactical analysis support on SOC;</li> <li>○ Provide analytical contributions to improve the intelligence picture in different crime areas;</li> <li>○ Prepare and support prevention materials and campaigns;</li> <li>○ Develop expertise in the serious and organised crime mandated areas;</li> <li>○ Coordinate demand and development of new technical solutions;</li> <li>○ Coordinate R&amp;D involvement;</li> <li>○ Organise major stakeholder events and conferences;</li> <li>○ Coordinate partnerships and stakeholder networks.</li> </ul>
<p><b>Operations - Commodities and Organised Crime Networks</b></p>
<p><i>Operations on Drugs</i></p> <ul style="list-style-type: none"> <li>○ Disrupt the Organised Crime Groups (OCGs) involved in cocaine trafficking and distribution (AP Cola);</li> <li>○ Disrupt the OCGs involved in heroin trafficking and distribution (AP Heroin);</li> <li>○ Disrupt the OCGs involved in synthetic drugs trafficking and distribution (AP Synergy);</li> <li>○ Disrupt the OCGs involved in Cannabis trafficking and distribution (AP Cannabis).</li> </ul>
<p><i>Operations on Top Organised Crime Groups</i></p> <ul style="list-style-type: none"> <li>○ Disrupt Mafia-structured OCGs originating in Italy and impacting other MS (AP ITOC);</li> <li>○ Disrupt Ethnic Albanian Organised Crime Networks (AP Copper);</li> <li>○ Disrupt Eastern European Organised Crime Networks (AP EEOC);</li> <li>○ Disrupt Outlaw Motorcycle Gangs (AP Monitor).</li> </ul>
<p><i>Operations on Weapons &amp; Explosives</i></p> <ul style="list-style-type: none"> <li>○ Disrupt illicit trafficking in firearms and explosives (AP Weapons &amp; Explosives).</li> </ul>
<p><b>Operations - Economic and Property Crime</b></p>
<p><i>Operations on Fraud</i></p> <ul style="list-style-type: none"> <li>○ Disrupt the capacity of OCGs and specialists involved in excise fraud (AP Smoke);</li> <li>○ Disrupt the capacity of OCGs and specialists involved in Missing Trader Intra Community fraud (AP MTIC);</li> <li>○ Disrupt the capacity of OCGs involved in fraud (AP Apate);</li> <li>○ Disrupt the capacity of OCGs and specialists involved in sport corruption (AP Sports corruption);</li> <li>○ Disrupt the capacity of OCGs involved in environmental crime (AP EnviCrime).</li> </ul>
<p><i>Operations on Counterfeiting</i></p> <ul style="list-style-type: none"> <li>○ Disrupt the OCGs involved in the production and distribution of counterfeit goods violating health, safety and food regulations, and those producing sub-standard goods (AP Copy);</li> <li>○ Disrupt the OCGs involved in Euro Counterfeiting (AP Soya);</li> <li>○ Manage the Intellectual Property Crime Coordination Coalition (IPC<sup>3</sup>) established in cooperation with EUIPO; disrupt intellectual property crime through (i) interdiction and investigation of Organised crime groups and networks, (ii) outreach to the public and to law enforcement through awareness raising and delivering training on</li> </ul>

**Europol Public Information**

intellectual property crime and, (iii) effective and efficient leverage of available resources, skills and capabilities of all stakeholders (AP Copy).
<i>Operations on Property Crime</i>
<ul style="list-style-type: none"> <li>o Combat organised property crime committed by Mobile Organised Crime Groups (AP Furtum).</li> </ul>
<b>European Migrant Smuggling Centre and Trafficking in Human Beings</b>
<i>Operations on Facilitation of Irregular Migration</i>
<ul style="list-style-type: none"> <li>o Act as the EU Centre of expertise on migrant smuggling;</li> <li>o Proactively support MS to target and dismantle organised crime networks involved in migrant smuggling (AP Migrant smuggling, JOT Mare and dedicated operational and technical support);</li> <li>o Improve and strengthen the investigation and analytical support on the spot with the help of Europol Mobile Investigation Support Teams (EMIST) and Europol Mobile Analytical Support Teams (EMAST);</li> <li>o Monitor migration flows and their impact on crime; highlight links between migrant smuggling and other crime areas and terrorism;</li> <li>o Be the central Europol contact point in the EU Regional Taskforce (EU RTF).</li> </ul>
<i>Operations on Trafficking in Human Beings (THB)</i>
<ul style="list-style-type: none"> <li>o Disrupt OCGs involved in intra-EU human trafficking and human trafficking from the most prevalent external source countries for the purposes of labour and sexual exploitation; including those groups using legal business structures to facilitate or disguise their criminal activities (AP Phoenix).</li> </ul>

**2019 Objectives**

A.3.1 Improve procedures and operational approach to foster Europol’s support to MS investigations against organised crime.

Actions	<p>Promote to and support the EU MS in applying Europol’s Standard Operating Procedure on the Selection of High Value Targets and Establishment of Operational Task Forces (OTF).</p> <p>Enhance cross-border operational cooperation and information exchange by establishing an OTF working environment (i.e. temporary teams consisting of representatives of the Member States and Europol, based on a multi-disciplinary approach) to carry out a specific project consisting of intelligence and investigative activities against HVTs.</p> <p>Provide dedicated support to EU-financed projects targeting the identification, infiltrating and dismantling of mafia-type organised crime structures and criminal networks through intelligence, analysis and forensic tools.</p> <p>Based on the 2018 EU Strategy for the Western Balkans and its priority areas for the mandate of Europol, draft and implement an Operational Action Plan defining Europol’s response to organised crime affecting EU MS from the Western Balkans and related cooperation arrangements with relevant non-EU countries.</p>
Expected results	Improved coordination of action and operational cooperation in the EU against organised crime groups constituting the highest risk for the internal security.

**Europol Public Information**

Europol's enhanced ability to respond effectively to investigations requiring rapid reaction.

A.3.2. Ensure the implementation of the objectives of the Malta Implementation Plan in the fight against organised crime related to migrant smuggling and THB.

**Actions**

Support MS in the identification of High Value Targets (HVTs) involved in migrant smuggling activities and develop dedicated intelligence gathering activity on HVTs active in the relevant hubs.

Apply the Rotating Expert Model (i.e. flexible, short-term operationally based deployments of EMSC experts) in cooperation with the EEAS to support the EU MS organised migrant smuggling and THB investigations which are linked to the third countries.

Develop the Crime Information Cell concept with the European Union Naval Force Mediterranean (EUNAVFOR MED) to enhance the information exchange with EU CSDP civilian and military missions. Replicate the concept with other relevant cells.\*

Prepare to participate, on the basis of operational needs, in the Regional Cooperation and Implementation Platforms (RCIPs) in the MENA countries that would function as a base for operations and a gateway for information from various cooperation partners. Where feasible make use of available EU resources and representations in the MENA countries.

Further progress with the establishment of the Information Clearing House at Europol to enhance information exchange between EU MS law enforcement authorities and EU CSDP civilian and military missions and EU delegations in third countries. Set up the conditions allowing for increasing (near) live transmission of relevant data to Europol's databases.\*

Organise and coordinate action days focussing on embarkation points and other key logistical hubs (together with Frontex, Interpol and other relevant partners).

Provide training/awareness in selected MENA countries on Europol cooperation possibilities both in the field of migrant smuggling and THB in accordance with the staffing and budgetary resources at Europol's disposal and in coordination with CEPOL.

**Expected results**

Europol is able to base its operational support functions on real time information and to respond swiftly to changing organised migrant smuggling and THB trends.

MS investigations receive better and extended support in relation to dismantling of organised crime groups active in migrant smuggling and trafficking in human beings.

## Europol Public Information

A.3.3. Undertake and support further improvements in the strategic and operational approach followed by the MS and Europol in targeting the reduction of drugs supply.

### Actions

Establish a European Drugs Unit within Europol with enhanced working processes to ensure proactive collection of intelligence and efficient targeting and prioritisation.

Reinforce the cooperation with EMCDDA to fulfil the joint undertakings in the area of drug supply reduction, in line with the revised Europol's Drug Strategy<sup>14</sup>.

Further develop the functions of the Drug supply reduction Programme Board consisting of the representatives of the EU MS, EU Commission, Eurojust and EMCDDA, and ensure the implementation of the "Action Plan for Enhancement of Drug Crime Investigations".

Prepare and publish a new handbook on chemicals used in the production of drugs.

In coordination with the competent national LEAs develop cooperation with Antwerp and Rotterdam maritime ports which are the most vulnerable and targeted ports in the EU for drug trafficking in order to increase the quality of the collected intelligence and the efficiency of the counter measures.

Continue enhancing the collaboration with the MS and relevant partners for establishing task forces for conducting joined investigations and operations on high prioritised drug cases.

Assess Europol's potential role in respect to the EU funded development of technological solutions for the forensic and surveillance services needed for the investigation of cross-border drug trafficking. Explore the possibilities to increase collaboration with the private sector with regard to such technological developments.

Enhance Europol's strategic analysis functions in respect to the drug crimes in order to ensure that Europol would have capacities to provide the MSs with information which is needed for the intelligence led policing in respect of drug crime prevention.

Ensure that MS and Europol receive increasing access to up-to-date intelligence through the setting-up of public-private partnerships such as with relevant EU courier / parcel post companies and aviation authorities concerning trafficking of drugs or precursors, and suspicious flights and air couriers.

Conduct regular communication and awareness campaigns highlighting EU drugs threats as well as the EU efforts for combating this phenomenon, in coordination with EMCDDA.\*

### Expected results

Reduction of the drug supply is based on real time intelligence enabling timely response to emerging organised crime trends.

Improved coordination and efficiency of action in the EU against common and high level priorities in the area of drug supply reduction.

<sup>14</sup> Toward a Bold Europol Response to Drugs in Europe (EDOC-#892562)



**Europol Public Information**

MS investigations in relation to drug crime receive better and extended support.

**A.3.4. Strengthen the fight against counterfeiting and intellectual property crime.**

**Actions**

Further build up the operational and technical support to the MS' fight against Intellectual Property Crime through the Intellectual Property Crime Coordinated Coalition (IPC3) in cooperation with the European Union Intellectual Property Office (EUIPO).

Intensify the utilisation of special police techniques in IP investigations and focus on OCGs and money trail. Initiate establishment of links with existing structures for collaboration on intellectual property rights enforcement and with intermediaries (e.g. shipping and advertisement companies).

Increase proactive screening of the internet for webpages selling counterfeited goods in order to create referrals for MS competent authorities.

Expand partnerships with public and private sector agencies, associations and academia to produce risk assessments and trend analysis reports.

Support the development, provision and coordination of training to competent authorities in the area of intellectual property crime, in cooperation with CEPOL.

Initiate new cooperation arrangements with the European Central Bank and launch a joint project under the auspices of AP Soya to enhance the fight against Euro Counterfeiting in the online domain.\*

**Expected results**

Improved coordination of action in the EU against common priorities in the area of counterfeiting and intellectual property crime.

MS investigations in relation to counterfeiting and intellectual property crime receive better and extended support.

**A.3.5 Strengthen the fight against organised crime groups involved in fraud activities.**

**Actions**

Initiate a new project under AP MTIC to monitor, identify and report on Alternative Banking Platforms (ABPs) being used to funnel the proceeds of MTIC fraud towards out of the EU.

Establish a Memorandum of Understanding with the Intra-European Organisation of Tax Administrations (IOTA) for cooperation in the field of MTIC fraud prevention and detection.

Initiate a new joint project with the EUIPO under AP Apatate to counter acquisition frauds targeting Intellectual Property Offices and trade-marks and design services in the EU.

Enhance under AP Sports Corruption Europol's capacity to receive increasing access to up-to-date intelligence through the setting-up of new public-private partnerships with relevant sports monitoring agencies and NGOs.

## Europol Public Information

---

	<p>Review the role of Europol under AP Envicrime in supporting the EnviCrimeNet (the informal network connecting police officers and other crime fighters in the field of environmental crime).</p> <p>Increase cooperation with Frontex in the maritime domain in order to enhance the detection of environmental crime related to illegal fisheries and marine pollution.</p>
Expected results	<p>Exchange of information, operational cooperation and situational awareness on financial and economic crimes are further enhanced which leads to increasing prevention and detection of such crimes within the EU.</p> <p>MS investigations in relation to fraud crime receive better and extended support.</p>
<hr/> <b>A.3.6 Strengthen the fight against organised property crime.</b> <hr/>	
Actions	<p>Organise think tank meetings on specific organised property crime phenomena (e.g. jewellery theft, theft of GPS devices from agricultural equipment, theft of luxury bicycles, etc.) to develop a more in depth picture of the crime area and build investigative strategies adapted to the targeted Mobile Organised Crime Groups.</p> <p>Develop Europol's proactive activities, e.g. utilisation of new technologies such as Face recognition and acquiring new tools such as jammer detectors, to identify individuals and criminal organisations/networks.</p> <p>Support the organisation of a Joint Action Day targeting various modalities of motor vehicle crime, including smuggling of stolen vehicles, and associated document fraud.</p> <p>Initiate a new project under AP Furtum to facilitate the faster identification of stolen vehicles by providing the MS with a direct access to the database on the Forensic Aid for Vehicle Identification (FAVI) via the EPE. Increase awareness about the new possibilities.</p> <p>Establish Europol's involvement in a novel public/private sector partnership to create a global database for stolen watches and luxury items. Provide MS with direct access to the database via the EPE and raise awareness about the new possibilities.</p> <p>Organise a Pickpocket Conference at Europol to discuss on-going operations, new modus operandi and prevention measures.</p>
Expected results	<p>Improved access to information and coordination of action in the EU in the area of organised property crime.</p> <p>MS investigations in relation to organised property crime receive better and extended support.</p>

---

(\* The level of implementation of actions marked with an asterisk throughout the Work Programme depends on the availability of additional resources.)

### Europol Public Information

Indicators	Latest result Q3 2018	Target 2019
<i>Operations supported related to SOC</i>	612	800
<i>Operational reports delivered related to SOC</i>	3,445	4,600
<i>Satisfaction with operational support and analysis in the area of SOC</i>	8.7	8.5
Number of cases where High Value Targets were identified	-	10
Operations supported by EMSC	134	130
<i>On-the-spot support deployed related to EMSC (days)</i>	885	700
Volume of content assessed by the EU IRU related to migrant smuggling	801	900
% of successful referrals by the EU IRU related to migrant smuggling	93%	75%
Operations supported related to drugs	148	200
Operations supported related to OCGs	75	100
Operations supported related to weapons and explosives	56	80
Operations supported related to counterfeiting	38	45
Operations supported related to fraud	81	100
Operations supported related to organized property crime	85	90

## A.4. Combating Cyber Crime

### Overview

The European Cybercrime Centre (EC3) was launched at Europol in January 2013 to strengthen the EU law enforcement response to cybercrime by delivering operational and investigation support to the services in the Member States competent to fight organised crime and terrorism. The Centre is tasked to focus on three main areas, namely:

- Cybercrimes committed by organised groups, particularly those generating large criminal profits such as online fraud,
- Cybercrimes which cause serious harm to their victims, such as online child sexual exploitation and
- Cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the European Union.

The Communication of the Commission on *The EU Internal Security Strategy in Action*, further describes the role of the cybercrime centre as follows:

- Strengthen and integrate operational and analytical capacities for cybercrime investigations in the Union, including a reinforcement of the cooperation with Member States, international partners and the private sector;
- Evaluate and monitor existing preventive and investigative measures in the area of cybercrime;
- Support the development of training and awareness-raising initiatives of law enforcement, judicial authorities and the private sector;
- Facilitate the reporting of cybercrimes and simplify subsequent processing of the information by Member States' law enforcement via interlinking national cybercrime alert platforms to a central European cybercrime alert platform;
- Improve cooperation with the European Network and Information Security Agency (ENISA) as well as national/governmental Computer Emergency Response Teams (CERTs) on law enforcement relevant aspects of cyber security.

In addition, the Commission's Communication on *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* from September 2017 underlines the importance that Europol should further develop its cyber forensic capability and reinforce the support to investigations on the Dark Web. Another major priority is to increase the technological focus on the abuse of encryption by criminals which creates significant challenges in the fight against serious and organised crime, cybercrime and terrorism.

### Recurrent actions

Main tasks
<p><i>Provision of Operational Support</i></p> <ul style="list-style-type: none"> <li>○ Serve as the EU law enforcement hub for collecting, storing, processing, analysing and exchanging information and criminal intelligence of relevance for cybercrime and cyber-enabled (e.g. Dark Web) investigations;</li> <li>○ Provide cross-checking, operational analysis, support, coordination and de-confliction to MS cybercrime investigations in the areas of cyber-dependent crimes, transnational payment fraud, child sexual exploitation, Dark Web, and cross-cutting crime enablers;</li> <li>○ Support multidisciplinary cyber investigations and facilitate the secure information exchange with key public and private partners;</li> </ul>

**Europol Public Information**

<ul style="list-style-type: none"> <li>○ Provide an on-the-spot service by deploying cyber analysts and/or specialists to support ongoing operations;</li> <li>○ Provide 24/7 support to MS for immediate reactions to urgent cyber cases and cyber crises situation via stand-by duty and the Law Enforcement Emergency Response Protocol (LE ERP).</li> </ul>
<p><i>Document Forensics</i></p> <ul style="list-style-type: none"> <li>○ Support MS investigations with regards to false documents, counterfeit currency and printing devices;</li> <li>○ Provide forensic services, reports and examinations, including forensics services accredited to ISO17020:2012;</li> <li>○ Support MS investigations with video enhancement analyses;</li> <li>○ Share the expertise and provide training in false document and currency identification;</li> <li>○ Support EU Policy Cycle priorities on document fraud and related investigations;</li> <li>○ Assist in the dismantling of clandestine print shops.</li> </ul>
<p><i>Digital Forensics</i></p> <ul style="list-style-type: none"> <li>○ Provide forensic services, including expertise, examination and training in regard to digital forensics, mobile devices, computers and ICT infrastructure, such as the Forensic IT Environment;</li> <li>○ Provide technical support to MS investigations obstructed by encryption via the dedicated Decryption Platform;</li> <li>○ Actively support MS in overcoming the technical challenges to their cyber and cyber-facilitated investigations, by identifying suitable tactics, developing dedicated tools, and sharing best practices to respond to the emerging operational needs (e.g. cryptocurrencies/Blockchain and Big Data analysis, etc.);</li> <li>○ Provide support and guidance in relation to covert digital activities;</li> <li>○ Develop community of experts in the relevant digital forensic areas;</li> <li>○ Deliver the annual Digital Forensic Investigator training course.</li> </ul>
<p><i>Strategy and Outreach</i></p> <ul style="list-style-type: none"> <li>○ Facilitate the multi-disciplinary interaction between partners and stakeholders, including Advisory Groups, Cybercrime Prevention network, Internet Governance network and the Academic Advisory network, in the prevention and combating of cybercrime within the broader cyber security ecosystem;</li> <li>○ Continually improve the management of EC3's growing network of external partners;</li> <li>○ Foster and facilitate the preparation and delivery of standardised prevention and awareness campaigns in relation to the cybercrime mandated areas;</li> <li>○ Interact with law enforcement representatives in the EU, industry and academia to develop and present collective views in relation to EU policy making and legislative process;</li> <li>○ Represent and promote the views of public safety and law enforcement agencies in the global discussion on Internet Governance;</li> <li>○ Coordinate and support the demand, development and delivery of comprehensive cybercrime training under the umbrella of a Training Governance Model at EU level;</li> <li>○ Collect, analyse and manage strategic intelligence, and further develop expertise with a view to supporting pro-active and innovative approaches;</li> <li>○ Interact with partners, including other EU entities, to facilitate effective cooperation in the development and delivery of strategic analysis, advisory threat intelligence and forward-looking products;</li> <li>○ Identify common challenges to combating cybercrime in collaboration with Eurojust;</li> <li>○ Coordinate the demand and development of new technical solutions and products, including R&amp;D with the Forensic Experts Forum and other relevant stakeholders;</li> <li>○ Coordinate and provide advice to R&amp;D priorities at national and EU level, particularly in relation to EU funding programs, if and where appropriate.</li> </ul>
<p><b>Thematic operations</b></p> <p><i>Cyber Intelligence for Operations</i></p>

## Europol Public Information

- Collect information on cybercrime and cyber-facilitated crime threats and trends from a wide array of public, private and open sources;
- Support EU MS by identifying new modi operandi and identifying investigative opportunities through pro-active analysis and exploitation of the contributed data;
- Provide knowledge products with regard to technology and new criminal modi operandi online;
- Monitor new technological developments impacting cyber and traditional crimes and build expertise;
- Support EU MS with OSINT analysis and expertise;
- Provide operational, tactical and strategic support in the area of crypto-currency;
- Facilitate the operational collaboration between cyber law enforcement and cyber security/network and information security community (e.g. CERTs/CSIRTs, NIS, ENISA, CERT-EU, etc.).

### *Operations on Cyber-Dependent Crimes*

- Provide operational coordination and support to Member States' investigations in regard to cyber-dependent crimes of greatest concern (AP Cyborg);
- Focus on preventing and combating cyber criminality affecting critical infrastructure and network and information systems;
- Focus on investigating, targeting and disrupting cybercrimes associated with organised groups generating greatest harm and/or large criminal profits and cybercrime-as-a-service schemes;
- Provide a dedicated, secure and automated malware analysis platform to MS through the Europol Malware Analysis Solution (EMAS).

### *Operations on Child Sexual Exploitation*

- Support the EU MS in preventing and combating all forms of criminality associated with the sexual exploitation of children (AP Twins);
- Tackle forms of criminal online behaviour against children, such as grooming, self-generated indecent material, sexual extortion and coercion, and web live streaming;
- Fight distribution of child sexual exploitation material including preventing, intercepting and stopping the sharing through peer-to-peer networks, commercial platforms, and the Dark Web, as well as addressing the commercial sexual exploitation of children via the European Financial Coalition (EFC) chaired by EC3;
- Enhance the Victim Identification efforts, including the development of the Image and Video Analysis Solution (IVAS) and hosting of the Victim Identification Taskforce to foster cooperation and pooling of expertise from different police agencies and Interpol;
- Tackle the phenomenon of transnational child sex offenders by supporting the EU MS in detecting and intercepting of travelling child sexual offenders, among others, with the help of the newly adopted EU PNR Directive;
- Deliver training courses on Victim Identification and Combating Online Sexual Exploitation of Children;
- Update regularly EU MS experts on intelligence relating to online platforms being set up, maintained or abused for the purpose of child sexual exploitation;
- Enable the establishment of dedicated information flows and communication mechanisms to receive, process and disseminate information on suspected child sexual exploitation online from pertinent non-law enforcement actors to the relevant competent authorities in the EU MS in a secure and time-sensitive manner.

### *Operations on Non-Cash Payment Fraud*

- Support the MS in combating criminal networks in regard to various types of online payment fraud (card-not-present fraud), including e-commerce fraud, and coordinate large-scale multi-sector joint operations against it (AP Terminal);
- Tackle forms of payment fraud such as skimming (duplication of a card's magnetic strip often through devices hidden within compromised ATMs and Point-Of-Sale terminals) and cyber-enabled non-cash payment types of fraud;
- Execute the joint action week on carding (unauthorised use of credit or debit card data to purchase products and services in a non-face-to-face setting, such as e-commerce websites);

**Europol Public Information**

<ul style="list-style-type: none"> <li>o Execute the joint operational action against telecom fraud, in collaboration with law enforcement, judiciary and relevant private partners;</li> <li>o Support the MS in addressing new emerging trends and criminal Modi Operandi (e.g. payment process compromise incl. intrusion into processing of payment card systems, ATM malware, Black Box attacks, compromise of Near Field Communication transactions, etc.);</li> <li>o Coordinate the detection, identification, dismantling, prosecution and prevention of money muling, together with key partners (Eurojust, financial sector, etc.);</li> <li>o Facilitate cooperation among LEAs, the private sector and regulators (the European Central Bank at the European level and National Banks at a domestic level);</li> <li>o Actively engage with priority regions to address payment fraud migration;</li> <li>o Deliver the annual training course on Payment Card Fraud Forensics and Investigations.</li> </ul>
<p><i>Operations on Online Trade in Illicit Goods and Services</i></p> <ul style="list-style-type: none"> <li>o Support the MS in combating criminal networks in regard to the administration and moderation of Dark Web related activities;</li> <li>o Enhance the intelligence picture of the online trade in illicit goods and services online, in particular on the Dark Web;</li> <li>o Provide a common law enforcement response to criminality on the Dark Web by combining EC3's expertise with the crime specific knowledge of other Europol operational teams;</li> <li>o Strengthen the operational coordination, de-confliction, prioritisation and investigation of Dark Web related crimes at an international level;</li> <li>o Support the planning and execution of joint technical and investigative actions;</li> <li>o Further develop knowledge and expertise on tools, tactics and techniques for conducting Dark Web investigations;</li> <li>o Support the delivery of training related to Dark Web investigations.</li> </ul>
<p><i>J-CAT</i></p> <ul style="list-style-type: none"> <li>o Host and support the work of the Joint Cybercrime Action Taskforce (J-CAT) composed of Cyber Liaison Officers from closely involved Member States, non-EU law enforcement partners and EC3;</li> <li>o Stimulate and facilitate the joint identification, prioritisation, preparation and initiation of cross-border investigations and operations by the J-CAT partners;</li> <li>o Pro-actively drive intelligence-led, coordinated action against jointly identified, key cybercrime threats and top targets;</li> <li>o De-conflict and identify synergies for joint operational activities with the other global cybercrime taskforces and key cyber operational centres (NCFTA and INTERPOL) towards optimising resources and the effectiveness of operations;</li> <li>o Facilitate the collaboration and operational engagement with Eurojust on cybercrime cases via the dedicated Eurojust cyber SNE;</li> <li>o Maintain an attachment scheme to the J-CAT within which non-Taskforce members of operational relevance would be temporarily working with the J-CAT on a case-basis.</li> </ul>

**2019 Objectives**

<p>A.4.1. Accelerate Europol's capabilities to provide support to MS' investigations in the area of cybercrime-related EU Policy Cycle priorities 2018-2021.</p>	
<p>Actions</p>	<p>Fully establish the Europol Dark Web Team at Europol – a new dedicated capability to deal with the growing number of investigations related to online trade in illicit goods and services with cross-crime elements.*</p> <p>Develop new tactics, tools and techniques needed by EU LEAs to combat criminality on the Dark Web (e.g. improved data collection, analysis, network investigations, etc.).*</p>

## Europol Public Information

---

Organise Joint Action Days on addressing criminality on the Dark Web by focusing on top marketplaces, cross-crime multi-disciplinary action and crime-specific operations.

Set up specific cybercrime-related taskforce-based operational actions in the area of child sexual exploitation with a focus on Victim Identification, Travelling Child Sex Offenders, etc.

Draw upon the new EU PNR Directive to complement the Global Airline Action Days operations and the operational and strategic efforts related to Travelling Child Sex Offender by enriching the intelligence picture on key targets.

Optimise the possibilities for EC3 to facilitate the law enforcement response to non-cash payment fraud, in line with the new Non-Cash Payment Fraud Directive<sup>15</sup> and the Europol Regulation provisions for cooperation with private parties.\*

Assess the impact of cyber-facilitated business process compromise (e.g. malware driven CEO payment fraud) and identify operational support opportunities.\*

Enhance the capabilities of the Europol Malware Analysis Solution (EMAS) for ATM malware analysis.\* Assess the requirements for adding technical solution and expertise on malware virology/malware DNA and reverse engineering.\*

Arrange for Europol's participation in the Malware Information Sharing Platform (MISP)<sup>16</sup> in order to enrich the agency's intelligence picture with data collected by the Computer Security Incident Response Teams (CSIRTs).\*

Develop an EC3 OSINT platform in order to enhance operational information with data collected from open sources.\*

Establish a cryptocurrency platform where LEA can query open source blockchain.\*

Implement an accreditation system for EU LEA to connect to non-public WHOIS information database held by domain registries and registrars.\*

Actively contribute to the Horizontal Expert Groups (HEG) under EMPACT document fraud priority to establish coordinated support in the area of document fraud.

Develop Europol's capability to recover criminal data from vehicles\* and Digital Video Recorder (DVR) devices. Further improve the capability for recovering data from damaged or destroyed portable devices.

---

### Expected results

Enhanced role of Europol in Dark Web investigations.

Advanced OSINT and cryptocurrency support to MS' cyber and cyber-enable investigations.

MS receive better and extended analytical, technical and forensic support to their cybercrime related investigations.

---

<sup>15</sup> Subject to adoption of the Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment (COM/2017/0489 final)

<sup>16</sup> <http://www.misp-project.org/>



## Europol Public Information

A.4.2. Further develop Europol's capability for recovering encrypted criminal data and utilise the agency's potential to perform as a European centre of expertise on decryption.

Actions	<p>Create a second tier of decryption system in cooperation with the Joint Research Centre (JRC).</p> <p>Continuously monitor new trends in the use of encryption by criminals and explore different investigative opportunities and best practices in addressing the issue.</p> <p>Increase the cooperation with ENISA to identify, assess and define solutions to address the criminal abuse of encryption and online anonymity.</p> <p>Contribute to the capacity building efforts for law enforcement to obtain and handle digital evidence using techniques such as live data forensics or gathering contextual information in support of the decryption process.</p> <p>Develop a Decryption Experts group with relevant stakeholders.</p> <p>Further develop Europol's capability for retrieving data from password protected mobile devices.</p>
Expected results	<p>Increased capacity and functionalities of Europol's Decryption platform.</p> <p>MS investigations receive better support and expertise with regards to the criminal abuse of encryption and online anonymity.</p> <p>Coordinated EU LEA strategy on tackling the criminal abuse of encryption and associated challenges.</p>

A.4.3. Foster international cooperation and identify joint activities to address common challenges in the cybercrime and cyber-enabled crime area in a unified manner.

Actions	<p>Further engage with key cyber intelligence centres and cyber operational international taskforces (such as National Cyber-Forensics &amp; Training Alliance, International Cyber Crime Operations Summit (ICCOS), etc.) in order to facilitate the alignment, de-confliction and operational cooperation. *</p> <p>Expand the operational and strategic collaboration on payment fraud migration and card-not-present fraud with Latin America, the Eastern Partnership countries and identified key countries in Africa.</p> <p>Initiate the establishment of a secure technical interface to enable bi-directional communication on non-cash payment fraud cases and exchange of crime-relevant information with key private sector partners, in line with the Europol Regulation.*</p> <p>Undertake actions to further strengthen the role of LE in cyber security, cyber resilience and deterrence, including supporting the definition and development of information sharing interfaces and processes at strategic and tactical level between the relevant partners such as ENISA, CERT-EU and EDA.</p>
---------	--

**Europol Public Information**

	<p>Organise a cyber exercise for EU LEA and key partners from the cyber security ecosystem to test the EU Law Enforcement Emergency Response Protocol.</p> <p>Actively participate in and support other pan-European/joint cyber exercises, focusing on the role of law enforcement.</p> <p>Together with the relevant partners, initiate and implement a technology watch function to pro-actively inform about criminal abuse of new technology while ensuring the consideration of the law enforcement angle in the process of development.</p> <p>Explore possibilities to establish partnerships with new industry sectors with a specialised focus on partners of relevance for Dark Web investigations, as well as energy and automotive. Create a fourth advisory group, if proved feasible.*</p> <p>Host the biennial expert meeting on technical investigations on printed devices.</p> <p>Explore possibilities for pro-active collaboration with key stakeholders on combating document fraud under the EMPACT document fraud priority.</p>
Expected results	<p>Improved joint operational activities with public and private partners of relevance.</p> <p>More effective levels of cooperation leading to better coordination and increased operational and strategic results.</p>

(\* The level of implementation of actions marked with an asterisk throughout the Work Programme depends on the availability of additional resources.)

Indicators	Latest result Q3 2018	Target 2019
<i>Operations supported related to cybercrime</i>	215	200
<i>Operational reports produced related to cybercrime</i>	662	1,000
<i>Satisfaction with operational support and analysis in the area of cybercrime</i>	8.9	8.5
Number of forensic jobs performed by EC3	1,834	2,000
Number of forensic examinations on printed materials (e.g. euro banknotes, brand labels, documents etc.)	8	15
Number of Europol Forensic Lab deployments on the spot by the EC3 Lab	11	10
Number of on the spot mobile device examination kit deployments in all crime areas	109	100

**Europol Public Information**

Indicators	Latest result Q3 2018	Target 2019
Number of files submitted to EMAS by MS	101,122	200,000
Number of malicious files identified through EMAS	52,924	150,000
Number of times decryption platform is used	18	20
Number of decryption platform successes	8	10
Success rate of decryption platform (%)	44%	50%
Number of child abuse victims identified as a result of investigations supported by Europol	-	10
Number of prevention campaigns organised	4	6
Number of cooperation agreements or working arrangements concluded with the private sector	7	5

## A.5. Counter-Terrorism

### Overview

The European Counter-Terrorism Centre (ECTC) was established within the organisational structure of Europol in January 2016. Against the background of the current security threat the EU is facing, the political direction and Europol's Strategy 2016-2020, the ECTC is expected to maximise operational, technical and overall information exchange capabilities in the area of counter-terrorism and ensure added value for EU Member States, as well as third party cooperation partners, namely by providing:

- An information hub for counter terrorism, with unique information and intelligence sharing capabilities for law enforcement authorities in EU Member States and beyond.
- Effective operational support, coordination and expertise for Member States' investigations, by developing and deploying a comprehensive portfolio of support services.
- Proactive mitigation of the use of social media for radicalisation purposes through terrorist and violent extremist propaganda, as well as cyber-terrorist attack scenarios and support to operational analysis.
- A central strategic support capability, to identify European wide counter-terrorism implications and promote outreach with relevant (international) partners.

### Recurrent actions

Counter-terrorism Operations
<p><i>Provision of Operational Support</i></p> <ul style="list-style-type: none"> <li>○ Coordinate criminal intelligence collection and management;</li> <li>○ Monitor law enforcement information flows on 24/7 basis;</li> <li>○ Manage CT-related operational information received from secondary security checks performed by the guest officer deployed at the hotspots;</li> <li>○ Perform in-depth analysis of CT information;</li> <li>○ Identify emerging threats and developments;</li> <li>○ Detect links between terrorism and organised crime in close cooperation with the other Europol centres;</li> <li>○ Provide operational support to MS in a wide range of terrorism-related areas and in the field of responding to a major terrorist crisis;</li> <li>○ Manage the CT JLT operational platform and the First Response Network;</li> <li>○ Support the deployments of Mobile office and other mobile toolkits;</li> <li>○ Provide technical/ forensic support on the spot;</li> <li>○ Provide support to court hearings;</li> <li>○ Organise operational meetings at Europol.</li> </ul>
<p><i>Thematic Operations</i></p> <ul style="list-style-type: none"> <li>○ Identify activities of terrorist groups listed by the Council of the European Union and by the Working Group on Terrorism (3rd Pillar) as posing a serious threat to the security of the EU and the Member States, and any associate criminal activities within Europol's mandate uncovered in the course of the investigations into these terrorist networks (AP Dolphin);</li> <li>○ Prevent and combat crimes committed or likely to be committed in the course of terrorist activities against life, limb, personal freedom or property, and related criminal</li> </ul>

**Europol Public Information**

<p>offences associated with terrorism perpetrated by individuals, groups, networks or organisations who evoke Islam to justify their actions (AP Hydra);</p> <ul style="list-style-type: none"> <li>○ Prevent or combat terrorism by sharing analysis on related travel activities to terrorist hotspots, e.g. conflict zones and training venues (AP Travellers);</li> <li>○ Support MS in the fight against impunity of War Crimes, Genocide, Crimes against Humanity. Streamline the gathering and processing of information at EU level and provide analysis and operational support (AP Core International Crimes).</li> </ul>
<p><i>Counter Terrorism Financing</i></p> <ul style="list-style-type: none"> <li>○ Deal with MS requests for data on financial payments linked to terrorism including in accordance with the EU-US Terrorist Finance Tracking Programme Agreement (TFTP);</li> <li>○ Verify the link to terrorism in requests for data on financial payments;</li> <li>○ Support MS' investigations targeting networks facilitating the financing of terrorist actions or organisations;</li> <li>○ Provide support, including information on financial transactional data, to all operations where there is a link to terrorism;</li> <li>○ Liaise with Europol's Financial Intelligence Unit and with the competent ESOCC and EC3 units to close information gaps.</li> </ul>
<p><b>Strategy &amp; Expertise</b></p>
<p><i>Strategy and Outreach</i></p> <ul style="list-style-type: none"> <li>○ Administer and support the MS working group which aims at providing MS' strategic guidance to the ECTC and enhancing the info exchange related to Foreign Terrorist Fighters;</li> <li>○ Contribute to specific ECTC developments such as improving connectivity of relevant systems and tools; closing the intelligence gap between terrorism and organised crime;</li> <li>○ Reinforce the outreach to MS security services, within the remit of the regulatory frameworks at national level and in coordination with Counter Terrorism Group (CTG) members, in line with the counter-terrorism policy developments at EU level and by fully respecting the sole responsibility of Member States for national security;</li> <li>○ Provide support on drafting reports on strategic developments in terrorism threats, including trend analysis, early warnings, the 6-month high profile Outlook on developments in Jihadist terrorism and the annual high profile TE-SAT report;</li> <li>○ Cooperate with EU institutions and agencies and international organisations on CT matters;</li> <li>○ Participate in and contribute to the work of the High-Level Commission Expert Group on radicalisation;</li> <li>○ Oversee the establishment and management of external relationships with law enforcement, academia, and private sector entities with a particular focus on stakeholders at policy level;</li> <li>○ Perform the role of CT Program Board secretariat in assistance to its Chair;</li> <li>○ Organise stakeholder events, including the ECTC Advisory Group meetings and conferences on online terrorist propaganda.</li> </ul>
<p><i>Modus Operandi Monitor (MOM)</i></p> <ul style="list-style-type: none"> <li>○ Identify new terrorist Modi Operandi;</li> <li>○ Raise awareness on new Modi Operandi to all relevant partners;</li> <li>○ Provide tailored newsfeeds on terrorism trends and other relevant information by means of daily and monthly reporting to MS;</li> <li>○ Undertake joint actions with all relevant partners on preventive measures.</li> </ul>
<p><i>CBRN/E</i></p> <ul style="list-style-type: none"> <li>○ Manage and administer the Europol Platform for Experts pages: <ul style="list-style-type: none"> <li>- EPE/EBDS (European Bomb Data System);</li> <li>- EPE/EEODN (European Ordnance Disposal Units Network);</li> </ul> </li> <li>○ Ensure the permanent secretariat and the continuity of the activities of EEODN;</li> <li>○ Liaise with AP Weapons and Explosives to track possible new threats, trends and modus operandi involving CBRN materials and Explosives;</li> </ul>

**Europol Public Information**

<ul style="list-style-type: none"> <li>○ Prepare strategic and technical reports on CBRN and Explosives;</li> <li>○ Deliver capacity-building initiatives for MS on CBRN and Explosives.</li> </ul>
<b>EU Internet Referral</b>
<p><i>Internet Monitoring and Referrals</i></p> <ul style="list-style-type: none"> <li>○ Perform scanning of social media and cyber environment, within the framework of prioritised areas (terrorism and illegal migration) or act upon MS' specific requests;</li> <li>○ Coordinate and share the identification tasks (flagging) of online terrorist and violent extremist content with a network of national counterparts;</li> <li>○ Maintain the joint capability of the Internet Referral Management Application (IRMA) and the Check the Web Portal which supports the referral activity and enables MS to share information on terrorist/violent extremist propaganda on the Internet via a secured line;</li> <li>○ Deliver operational and strategic products;</li> <li>○ Support the activities of the EU Internet Forum's Action Plan. Maintain a close dialogue with the internet industry in the framework of the Forum;</li> <li>○ Organise and coordinate Targeted Referral Joint Action Days in cooperation with experts from MS and online service providers (OSPs);</li> <li>○ Build a network of academics and researchers in terrorism, radicalisation, computer sciences, information technologies, social network analysis and other pertinent areas of social science.</li> </ul>
<p><i>Internet Investigation Support</i></p> <ul style="list-style-type: none"> <li>○ Deliver operational and strategic products;</li> <li>○ Provide operational support and support coordination of CT Internet-based investigations;</li> <li>○ Organise operational meetings;</li> <li>○ Support MS in connecting with online service providers and analysing the digital footprint of a target in CT investigations through the SIRIUS capability.</li> </ul>
<p><i>Technical Support and R&amp;D</i></p> <ul style="list-style-type: none"> <li>○ Provide technical support to the Referrals and Operations teams;</li> <li>○ Provide expertise on big data management and analysis to the ECTC;</li> <li>○ Establish a European centre of excellence, by strategically enhancing partnerships with cooperation partners and investing resources in Research &amp; Development;</li> <li>○ Act as an Innovation Hub for Europol and the EU MS in the field of counter-terrorism;</li> <li>○ Contribute to the Innovation work-stream within the Operations Directorate by investing on prototyping initiatives;</li> <li>○ Develop the SIRIUS Platform to support Internet-based investigations and cross border access to e-evidence;</li> <li>○ Develop projects together with the private sector and academia on new techniques and tools in the context of EU grant funding programmes.</li> </ul>

**2019 Objectives**

<p>A.5.1. Promote and facilitate greater information exchange in the area of counter-terrorism and provide better and extended operational support to Member States' investigations.</p>
--

<p>Actions</p>	<p>Continue strengthening Europol's capabilities to set up and maintain for the necessary duration ad hoc operational analytical and support task force(s), as well as on-the-spot deployments, for dedicated and comprehensive support to large-scale and possibly simultaneous transnational CT investigations.</p>
----------------	---

## Europol Public Information

---

Support the connection of all MS to CT SIENA. Promote the usage of SIENA as the main channel for MS CT information exchange (up to EU Confidential level).

Further build up Europol's CBRN expertise into a knowledge hub to support law enforcement authorities on CBRN security in line with the Commission's Action Plan on CBRN<sup>17</sup>. Optimise the use of Europol tools (notably EBDS and EEODN) to enhance the sharing of information and the collective knowledge on CBRN threats.

Continue developing and fine-tuning the Counter Terrorism Joint Liaison Team (CT-JLT) concept as a mature mechanism for proactive and intelligence-led coordinated action accelerating exchange of information and operational results. Ensure the consistent use of the Crisis Response Protocol for reaction in case of a terrorist event or an imminent terrorist threat.

Identify opportunities for cooperation between Counter Terrorism Group (CTG) members and Europol in areas of common interest, while fully respecting the sole responsibility of Member States for national security.

Continue enhancing cooperation with third countries<sup>18</sup>, in particular in the Western Balkans, Middle East and North Africa, in collaboration with the EMSC initiatives in the regions, in order to establish anti-terrorism partnerships. Support deployments of MS CT/security experts to the EU Delegations and civilian CSDP-missions.

Utilise opportunities for embedding ECTC staff members on a temporary basis into the Crime Information Cells or other multi-agency platforms dealing with particular CT related phenomena/subjects, with the aim to increase information gathering on the spot and enhance coordination.

Explore possibilities to further reinforce the on-the-spot support to MS by utilising the Guest Officers concept and potentially extend its scope to other crime areas.\*

Assist the MS in the development of the ECTC's Counter Terrorism Programme Board (CTPB) as a governance tool and steering mechanism<sup>19</sup> and support the implementation of the prioritised five CTPB strands of activity: Information exchange; Scalable operational support; CT online; CT and Organised crime touch points; and Scoping (new areas of work, such as Innovative Expertise).

---

### Expected results

Increased number of joint operations of Europol with the MS CT competent authorities.

Increased CT information exchange and strategic engagement with third countries.

MS CT investigations receive better and extended support, especially in the case of simultaneous operations and crisis response.

---

<sup>17</sup> EU Action Plan to strengthen chemical, biological, radiological and nuclear (CBRN) security, Oct 2017

<sup>18</sup> Subject to appropriate legal basis in place, i.e. international agreements or working arrangements

<sup>19</sup> In line with the Communication "Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders" - COM(2016) 602)

## Europol Public Information

### A.5.2. Expand the scope of the Cross Border Access to Electronic Evidence (SIRIUS) Project.<sup>20</sup>

Actions	<p>Develop digests and guidelines for publication on the SIRIUS platform to improve the knowledge of MS law enforcement and judicial authorities about how to access digital data from US-based OSPs. Provide translation of the platform content in several languages in order to increase the number of users.*</p> <p>Organise face-to-face events within the framework of the SIRIUS project aiming at improving the capability of MS law enforcement and judiciary authorities to produce quality information requests to OSPs.</p> <p>Support Internet investigations by providing ICT-based tools created by Europol in collaboration with MS and by sharing tools created by MS, when they wish to do so.</p> <p>Engage with US-based OSPs to secure their thorough support of SIRIUS activities. Strengthen the cooperation with Eurojust on delivering the joint SIRIUS activities and products.</p> <p>Collect and analyse data to deliver strategic reports on state of play, trends and challenges in the field of cross-border access to electronic evidence.*</p> <p>Increase SIRIUS's geographical scope by introducing guidelines on requesting data from OSPs based in countries other than the US.*</p> <p>Identify the tasks and responsibilities for Europol emerging from the Draft Regulation on E-evidence where the SIRIUS capability is mentioned as a possible EU platform for transmitting, facilitating the authentication of and gathering statistics on MS production or preservation orders to OSPs.</p>
Expected results	<p>Improved Europol's capabilities in the area of digital cross border investigations which leads to better and extended support to MS.</p> <p>Increased MS capacity to prepare effective digital data requests to OSPs and obtain electronic evidence.</p>

### A.5.3. Enhance Europol's internet referral capabilities for prevention and investigation in the context of the EU Internet Forum Action Plan to Combat Terrorist Online Content.

Actions	<p>Establish regular communication with Internet companies and increase efforts to reach out to smaller companies in order to raise awareness of terrorists' behaviour online and to help them build up resilience against the exploitation of their platforms.*</p> <p>Support Internet companies by providing expertise on the development of and training in new content detection and identification technology.</p> <p>Develop and test tools that allow for the detection of terrorist content across platforms.*</p>
---------	---

<sup>20</sup> Subject to receiving a grant from the European Commission and agreement on concrete priorities to be pursued by the SIRIUS project.



## Europol Public Information

---

Support the network of national IRUs to promote cooperation, coordination and the exchange of knowledge and best practices on referral capabilities, making use of Internet Referral Management Application (IRMA) as a pilot for a limited number of MS.\*

Develop an EU platform<sup>21</sup> to tackle illicit content online, through the merger of the IRMA and the Check the Web capabilities into a new technical environment applying new business rules. This platform should be accessible by all MS and relevant OSPs allowing for a real time two-way communication between the EU IRU, national IRUs and OSPs in the context of referrals and removal orders. Take preparatory steps if legal constraints<sup>22</sup> have been waived and the necessary resources for this new task have been provided.\*

Contribute to research on online terrorist propaganda to enrich the academic overview and facilitate Social Network Analysis.

---

Expected results	The referral process is managed efficiently. Cooperation with the private sector on content detection and referrals is growing. Increased number of terrorism-related online content is taken down.
------------------	---

<b>A.5.4. Implement the affiliation of the ATLAS Network of Special Intervention Units within the structure of Europol.*</b>
--

Actions	Establish the ATLAS Support Office (ASO) as a team directly attached to the head of the ECTC. Meet the technical requirements for setting up direct communication lines to the ATLAS network. Enable ASO to serve as the main interface of ATLAS Network with Europol's CT and SOC communities and support the establishment of links with other relevant law enforcement expert networks supported by Europol. Facilitate the exchange of strategic and operational expertise and practices with ATLAS in the various areas of combatting terrorism and serious and organised crime where relevant and in accordance with the applicable rules. Provide administrative and logistic support to the implementation of the ATLAS Annual Work Programme. Enhance the usage of the EPE of ATLAS.
---------	--

---

Expected results	Stable and more efficient administration of ATLAS through the use of Europol's existing structures and tools. Utilisation of linkages and synergies in terms of strategic and operational expertise between ATLAS and Europol and law enforcement networks.
------------------	--

---

<sup>21</sup> Subject to adoption of draft Regulation on preventing the dissemination of terrorist content online, COM(2018) 640 final.

<sup>22</sup> With regards to the ability of Europol to interact with private parties and in particular the OSPs.

### Europol Public Information

(\* The level of implementation of objectives or actions marked with an asterisk throughout the Work Programme depends on the availability of additional resources.)

Indicators	Latest result Q3 2018	Target 2019
<i>Operations supported related to CT</i>	469	500
<i>Operational reports produced related to CT</i>	1,358	1,700
<i>Satisfaction with operational support and analysis in the area of CT</i>	7.7	8.5
Number of EU MS/TP CT units configured to SIENA	47	48
Number of EU MS CT units connected to EIS	20	25
<i>SIENA messages exchanged by CT units</i>	41,580	55,000
<i>Number of accepted contributions related to CT</i>	4,845	7,000
<i>Number of EIS objects related to CT</i>	617,313	700,000
Number of MS contributing terrorism and foreign fighters related objects in EIS	21	26
Number of persons referred for secondary security checks	5,900	8,000
Number of hits resulting from secondary security checks	251	300
Number of platforms with suspicious internet content detected related to terrorism and violent extremism	-	180
Volume of content assessed by the EU IRU related to terrorism and violent extremism	21,152	20,000
Volume of referrals of suspicious internet content related to terrorism and violent extremism sent to OSPs by EU IRU	20,306	18,000
% of decisions for referral by the EU IRU related to terrorism and violent extremism	96%	90%
<i>% of successful referrals by the EU IRU of suspicious internet content related to terrorism and violent extremism</i>	67%	75%
Number of TFTP Art. 10 EU Requests for TFTP searches	111	175

## A.6. Provision of cross-cutting operational capabilities

### Overview

Analysis products are the basis of Europol's operational support to Member States. Ensuring their relevance and quality is essential and includes identifying the needs of Member States in terms of the type of analysis needed (e.g. strategic, thematic or operational), investing in the training of Europol's analysts, further developing and maintaining quality standards for analytical support and exploring new methods such as analysis of large or complex data sets.

Strong strategic intelligence is required to support the EU Policy Cycle and is aimed at increasing the impact on the set priorities by targeting serious international and organised crime. Europol's strategic and thematic analysis address the most important criminal threats in a coherent and methodological manner through optimum cooperation between the relevant services of the MS, EU Institutions and EU Agencies.

Europol supports the European Multidisciplinary Platform Against Criminal Threats (EMPACT) by providing administrative and logistical support to the EMPACT action plans and monitoring the EMPACT projects' progress. With the implementation of the Europol Regulation, the additional funds previously foreseen in the EMPACT Delegation Agreement are integrated into Europol's regular budget to allow Europol to financially support actions of the OAPs.

Special Tactics at Europol offers specialist law enforcement techniques assisting MS' investigations in any of the three priority areas of serious and organised crime, terrorism and cybercrime. Whilst remaining open to new developments, the following areas of knowledge and expertise are being currently supported: covert human intelligence sources, covert surveillance, counter-kidnapping and -extortion, hostage negotiation, specialist intervention, witness protection and fugitive active search.

Europol embedded in 2016 the FIU.net computer network and its components which facilitates the exchange of information between Financial Intelligence Units (FIUs) of the EU Member States. The provision of financial intelligence and operational support to MS within the areas of money laundering asset recovery, counter-terrorism financing and corruption is on the rise and financial intelligence is recognised as essential in all crime areas.

### Recurrent actions

#### Strategic intelligence – analysis

##### *Strategic analysis*

- Establish and implement a common, consistent and holistic approach towards strategic analysis across the Operations Directorate;
- Deliver strategic analysis products within the areas of serious and organised crime, cybercrime and terrorism, such as:
  - Serious and Organised Crime Threat Assessment (SOCTA) on particular intervals;
  - Internet Organised Crime Threat Assessment (i-OCTA)
  - EU Terrorism Situation and Trend Report (TE-SAT)
  - Regional and other Threat Assessments
  - Situation reports, Early Warning Notifications, Intelligence Notifications
  - Cyber Intelligence products
  - Reports planned in the EMPACT OAPs
  - Monthly Intelligence Summary Terrorism, reports on jihadist terrorism

**Europol Public Information**

<ul style="list-style-type: none"> <li>- Joint EMCDDA-Europol European Drug Markets Report</li> <li>- Other reports to support policy making at EU level and MS' decision making by delivering strategic recommendations based on an in-depth analysis of the major crime and terrorist threats facing the EU</li> <li>o Deliver thematic intelligence analysis products within the areas of serious and organised crime, cybercrime and terrorism;</li> <li>o Deliver open source monitoring reports based on the business need;</li> <li>o Organise the meetings of Advisory Groups (SOCTA, TE-SAT, best practices of analysis, etc.).</li> </ul>
<p><i>Analysis &amp; Training Coordination</i></p> <ul style="list-style-type: none"> <li>o Oversee the development, implementation and maintenance of efficient operational information management processes;</li> <li>o Monitor and enforce the standards related to the different process steps in the operational information management lifecycle to improve and maintain the quality and speed of Europol's services;</li> <li>o Ensure compliance with the data protection regulation and mitigate the risk of misconducts of sensitive data usage;</li> <li>o Coordinate Europol's training initiatives and respond to any new training needs of MS which may arise (incl. joint Europol/CEPOL training);</li> <li>o Coordinate and deliver training to operational staff.</li> </ul>
<p><b>Strategic Intelligence - direct support</b></p>
<p><i>Special Tactics</i></p> <ul style="list-style-type: none"> <li>o Act as the EU knowledge and expertise broker on specialist law enforcement techniques supporting MS investigations in the area of SOC, terrorism and cybercrime;</li> <li>o Develop and maintain expertise on informant handling, covert surveillance and controlled delivery, covert entry, counter-kidnapping and -extortion, fugitive active search, specialist intervention and witness protection;</li> <li>o Manage EU Most Wanted List containing high-profile internationally-wanted criminals;</li> <li>o Manage the High Risk Informant Database (HRDB) - a coded database allowing a more accurate risk assessment when working with foreign informants;</li> <li>o Manage the European Tracking Solution (ETS);</li> <li>o Manage the Virtual Command Post tool for live information exchange during operations;</li> <li>o Support the implementation of MASP and OAP through the involvement in joint investigations, large-scale operations and/or joint action days;</li> <li>o Organise strategic expert meetings, training, awareness raising and prevention activities in the area of knowledge management and in support of specialist networks.</li> </ul>
<p><i>EMPACT Support</i></p> <ul style="list-style-type: none"> <li>o Manage the Grant scheme which provides funding opportunities to EMPACT for the implementation of the priorities identified within the framework of the EU Policy Cycle, in consultation with the Council's Standing Committee on Operational Cooperation on Internal Security (COSI);</li> <li>o Facilitate the execution of the EMPACT projects by providing methodological, administrative and logistical support including support to drafting the Operational Action Plans, stakeholder management and preparing strategic and operational meetings;</li> <li>o Monitor and report on the EMPACT projects' progress. Provide recommendations;</li> <li>o Coordinate the planning of Joint Action Days;</li> <li>o Facilitate communication and collaboration between the crime priorities having common goals and/or interdependencies.</li> </ul>
<p><i>Passenger Name Records (PNR)</i></p> <ul style="list-style-type: none"> <li>o Implement Europol's role in the EU PNR architecture in line with the EU Directive;</li> <li>o Utilise effectively PNR data exchange provisions;</li> <li>o Provide support to the connectivity and data exchange among the Passenger Information Units (PIUs) in MS;</li> </ul>

**Europol Public Information**

<ul style="list-style-type: none"> <li>○ Provide support to PNR related projects;</li> <li>○ Participate in the informal working group on PNR.</li> </ul>
<p><i>Deployment Management and Support</i></p> <ul style="list-style-type: none"> <li>○ Manage and support large scale deployments by Europol, as well as deployments linked to first responses requested by MS;</li> <li>○ Coordinate, manage and support the guest officer deployments.</li> </ul>
<p><b>Financial Intelligence</b></p> <ul style="list-style-type: none"> <li>○ Process and handle financial intelligence information;</li> <li>○ Provide financial intelligence and operational support to MS and TP within the areas of money laundering, asset recovery, terrorism financing and corruption;</li> <li>○ Provide financial intelligence to the ESOCC, EC3 and the ECTC;</li> <li>○ Provide financial intelligence and operational support to EMPACT related activities;</li> <li>○ Support corruption investigations initiated by MS and promote the use of SIENA for the information exchange between anti-corruption authorities;</li> <li>○ Provide operational support on the spot, including for Joint Action Days (e.g. mobile office deployments);</li> <li>○ Manage and support the development of the FIU.net computer network;</li> <li>○ Organise the FIU.net Advisory Group meetings and dedicated workshops based on the Service Level Agreement (SLA);</li> <li>○ Organise on-site trainings on the FIU.net based on the SLA;</li> <li>○ Manage all EPEs relating to financial intelligence (FCIC, ALEFA, AMON, CARIN, EFIPPP, FIU net and FIU net AG) and handle their growth;</li> <li>○ Support the European Commission in the peer-reviews of the EU Asset Recovery Offices; contribute to the development of the Supra-National Risk Assessment and high-risk third countries assessment on money laundering and terrorism financing in the framework of the Expert group on Money Laundering and Terrorist Financing;</li> <li>○ Co-chair with the European Commission the ARO platform meetings;</li> <li>○ Support projects related to the fields of financial intelligence, money laundering, asset recovery, terrorism financing and/or corruption;</li> <li>○ Support and host the secretariats for the Anti-Money Laundering Operational Network (AMON) and the Camden Asset Recovery Inter-Agency Network (CARIN);</li> <li>○ Support the triparty Working Group on digital currencies (co-host secretariat jointly with Interpol and the Basel Institute);</li> <li>○ Conduct financial intelligence training and provide expertise in various events on money laundering and terrorism financing including by supporting CEPOL and UNODC courses on money laundering and financial investigations;</li> <li>○ Develop, promote and support the Europol Financial Intelligence Public Private Partnership;</li> <li>○ Contribute to policy development such as guidance drafting and standards revision when requested by the Commission;</li> <li>○ Collect EU MS requirements; prioritise and deliver strategic products.</li> </ul>

**2019 Objectives**

A.6.1. Contribute to the development of a common EU view on criminal analysis.	
Actions	<p>Facilitate and contribute to the establishment of standard EU definitions and quality criteria for analysis products. Agree with MS on common profiles for operational analysts.</p> <p>Develop in cooperation with MS common standards for analysis training.</p>

## Europol Public Information

---

	<p>Prepare the curriculum for and organise a Europol Summer School on criminal analysis.*</p> <p>Ensure the consistent application of definitions and criteria for the different types of analysis reports produced by Europol. Monitor the quality of the products and their correct classification.</p> <p>Provide technical advice on initiatives related to preparation of EU legislation on crime analysis, if any.</p>
Expected results	<p>Improved cooperation in the EU based on the agreed common view and standards on analysis leading to an increased operational impact.</p> <p>MS investigations receive better and extended analytical support.</p>

---

### A.6.2. Strengthen Europol's capabilities to deliver quality strategic reports.

Actions	<p>Ensure having in place up-to-date methodologies for each type of strategic analysis reports and their cross-organizational application.</p> <p>Optimize the processes of data collection. Promote the use of the common platform for exchanging data for strategic and thematic analysis, e.g. by adding an EPE targeting counter-terrorism and customs authorities.</p> <p>Further develop the concept of conducting strategic analysis by setting up joint analysis teams with MS analysts.</p> <p>Identify training needs and offer the necessary training opportunities for Europol's strategic analysts.*</p> <p>Identify further opportunities to extend the assessment of satisfaction to more strategic analysis products in order to better evaluate the impact that they have on MS practices and policies.</p> <p>Make full use of the opportunities of the newly available travel information for the strategic and thematic purposes.</p> <p>Produce the mid-term review of new, changing or emerging threats paying particular attention to the EU crime priorities defined in 2017.</p>
---------	---

---

Expected results	<p>Provision of timely and authoritative strategic intelligence products to MS on current criminal phenomena.</p> <p>Europol's strategic analysis products increasingly contribute to operational priority-setting within MS and the EU Policy Cycle, as well as policy making at MS and EU level.</p>
------------------	--

### A.6.3. Develop Europol's capabilities in the area of travel intelligence in line with the Travel intelligence Roadmap.\*

Actions	<p>Further develop and deliver specialised operational analysis reports on the basis of travel information and intelligence stemming from PNR and Advance Passenger Information (API).*</p>
---------	---

---

## Europol Public Information

---

	<p>Further develop and deliver strategic products reflecting crime specific characteristics concerning travel movements as input for the definition of targeting rules.*</p> <p>Support the development of innovative and interoperable solutions to meet the business requirements of the travel intelligence community.</p> <p>Create and gradually extend a dedicated liaison network with direct connection with relevant travel intelligence entities in the MS and other partnering countries.</p> <p>Organise a Travel Intelligence conference.</p> <p>Enhance cooperation with private partners relevant for the collection of travel intelligence.*</p> <p>Further complement the training material in regard to travel intelligence, including rule-based targeting and operational analysis. Contribute to the delivery of at least one training course for the analysis of travel related information in partnership with CEPOL.*</p> <p>Arrange for the possible acquisition of the database on suspicious travel agencies of the International Air Transport Association (IATA).</p>
Expected results	<p>Increased quality and completeness of Europol's intelligence picture with regards to travel information.</p> <p>MS investigations receive the required support for the processing of travel data and the results of such processing through Europol's operational products.</p>

---

A.6.4. Reinforce the provision of horizontal support to investigations by advancing the development of specialist law enforcement techniques.
---

Actions	<p>Continue improving and promoting the EU Most Wanted List webpage. Ensure close collaboration with MS aiming at timely publication of fugitives in particular after major events, such as terrorist attacks.</p> <p>Respond to the MS requests for setting-up EPEs for experts on Missing people, Cold-Cases, Disaster Victim Identification, Behavioural Investigative Advice and (crisis) hostage negotiation.</p> <p>Continue supporting EuNAT's actions [European Network of Advisory Teams – kidnapping, hostage taking and extortion] on both the 'Mass Hostage Taking' and 'Cyber Enabled Extortion' projects.</p> <p>Further develop a tool for de-conflicting online undercover operations.</p> <p>Conclude the agreement with the European Maritime Safety Agency (EMSA) and initiate the utilisation of maritime geospatial images for analytical purposes. Further research the options for using terrestrial geospatial images in cooperation with EU SatCen and the use of GOVSATCOM (secure governmental satellite communication) for law enforcement needs.*</p>
---------	--

---

## Europol Public Information

Progress with the elaboration of a sustainable solution for the High Risk Informant Database (HRIDB) subject to MS needs and further promote the tool's systematic use.\*

Support the rolling out and the use of the European Tracking Solution (ETS) by MS.\*

Utilise the progress of the working group on forensic automotive in order to advance the work of the Special tactics expert group on covert and near real time use of automotive data.

Actively seek opportunities for building synergies among the expert groups in the Special Tactics portfolio by bringing key representatives together to streamline developments and ensure compatibility (e.g. between ARGOS [Assembly of Regional Groups On Surveillance] and ISLE [International Specialist Law Enforcement] – covert entry on automotive; between ATLAS, EuNAT and ARGOS on hostage situation responses).

---

Expected results	Increased use and quality/functionality of Europol's special tactics tools.  MS investigations receive better and extended special tactics support.
------------------	---

A.6.5. Increase the provision of comprehensive financial intelligence to MS regarding money laundering, asset recovery, corruption and terrorism financing, including possible links to other criminal areas.

Actions	Enhance the exploitation of financial Intelligence at Europol via the enlargement of the Pan-European platform for suspicious transaction reports and cash seizures by inviting selected non-EU countries, Interpol and OLAF.  Follow up on the roadmap for a future FIU.net application ("FIU solution").* Support the development of the new system and organise the working group on the implementation process (under the umbrella of the FIU.net Advisory Group).  Organise the working group on the renegotiation of the Service Level Agreement between Europol and FIUs (under the umbrella of the FIU.net Advisory Group).  Identify opportunities for enhancing the cooperation among FIUs, law enforcement, customs and tax authorities in order to improve results in combatting money laundering, terrorism financing and serious and organised crime.*  Continue identifying lists of high value targets for other Policy Cycle priority areas for matching against FIU data.*  Continue intensifying the cooperation with financial institutions to increase the prevention, detection and reporting on suspicious transactions. Increase contacts with the European Banking Authority to identify opportunities for establishing structured cooperation in the future.*  Increase cooperation with the anti-corruption authorities. Explore the possibilities for establishing an Analysis Project on corruption.
---------	---

---



**Europol Public Information**

Engage with the Financial Action Task Force (FATF) on a structured basis and with the Egmont group in operational and strategic projects.

Support the BeCaNet project<sup>23</sup> creating a network of counter-terrorism financing experts and improving cooperation with private sector on CT matters.\*

Support the EBOCS project<sup>24</sup> which is aiming at establishing interconnection among business registers across borders in order to provide simplified and unified access to data on business ownership and control structures for financial analysis and investigation purposes.

Prepare for taking up any potential new task arising from the mapping exercise of FIUs led by the European Commission, including the possible establishment of an EU-FIU that would coordinate and assist Member States FIUs.\*

Support the establishment of a possible EU system for tracking terrorism financing (for transactions that are excluded from the EU-US TFTP agreement – notably the intra EU payments).\*

Utilise funding opportunities under the Horizon 2020 calls in order to initiate the development of a one-stop shop digital platform for financial investigators to query and cross-check different financial sources.\*

Assess effectiveness in Asset seizures on cases supported by Europol.\*

**Expected results**

Improved cooperation and joint undertakings with financial institutions leading to an increased operational impact.

MS investigations receive better and extended financial intelligence support.

Europol increasingly contributes to operational outcomes in the MS within money laundering and asset recovery investigations.

Investigations on organised crime and terrorism can better benefit from synergies between financial and criminal intelligence.

*(\* The level of implementation of actions marked with an asterisk throughout the Work Programme depends on the availability of additional resources.)*

Indicators	Latest result Q3 2018	Target 2019
Number of strategic analysis reports	59	40
Number of thematic analysis reports	202	250
Training activities for MS/TP	77	85

<sup>23</sup> The BeCaNet Project is the 'best practice, capacity building and networking initiative among public and private actors against Terrorism Financing', led by BKA, Germany.

<sup>24</sup> The EBOCS (European Beneficial Ownership and Control Structures) project is carried out with the financial support of the Internal Security Fund and is led by the European Business Register EEIG, Belgium.

**Europol Public Information**

Indicators	Latest result Q3 2018	Target 2019
Satisfaction of participants with training provided by Europol to MS	8.8	8.5
Number of Action Days	152	200
Operations supported with Special Tactics products/services	8	10
Operations supported with Travel Intelligence products/services	-	20
Number of accepted contributions to be processed related to Financial Intelligence	3,820	5,000
<i>Operations supported with Financial Intelligence products/services</i>	146	150
<i>Number of operational reports related to Financial Intelligence</i>	790	950
<i>Satisfaction with operational support and analysis in the area of Financial Intelligence</i>	8.4	8.5

## A.7. Governance, support and administration

### Overview

Europol strives for full compliance with principles of sound financial management, security, data protection and internal control standards as demonstrated by the overall positive findings resulting from the internal and external audit mechanisms. In the spirit of ensuring clear accountability towards its stakeholders, Europol also applies robust document and records management procedures and adheres to a systematic performance monitoring and reporting practice.

Europol implemented the staff reductions envisioned in the MFF 2014-2020 in the governance, support and administration related functions which at the same time faced an increased workload resulting from a growing demand for Europol's recurrent products and services as well as the assignment of additional tasks and staff to Europol. In this context of organisational growth and to materialise efficiency improvements, while at the same time further increasing the operational delivery, Europol adjusted its organisational structure and recurrently designed and reviewed its operational and support processes.

Europol has designed a multi-year transformation programme, next generation Administrative and Governance Environment (ngAGE) to renovate the way the agency operates in the administration domain, providing the organisation with modern and efficient solutions for corporate functions. The pursued target is to rationalise current diverse application landscape in support of streamlined corporate processes by leveraging a best-of-breed, composite architecture comprised of Commission-provided, in-house and cloud solutions integrated in a coherent fashion. In the meantime existing solutions will remain supported until their functions can be accommodated by ngAGE products. Where necessary bridging solutions will be put in place.

It remains a priority for Europol to ensure the best use of its resources, including developing the competencies of Europol staff with a view to enhancing its operational and strategic capabilities to support Member States.

### Recurrent actions

#### Coordination and accountability

##### *Cabinet*

- Coordinate and oversee the implementation of Europol's Strategy and Europol's External Strategy;
- Provide policy advice and prepare related policy documents;
- Support management and coordinate key corporate interests and new initiatives;
- Prepare and follow-up on the Directorate and Executive Deputy Directors meetings;
- Represent Europol at internal and external events;
- Provide administrative and logistic support to the Executive Director;
- Coordinate and support the activities of Europol Steering Group for Diversity & Inclusion;
- Coordinate academic requests reaching Europol.

## Europol Public Information

<p><i>Internal Control Coordination</i></p> <ul style="list-style-type: none"> <li>○ Coordinate all audit activities and Europol's response to audit activities and findings from the ECA, the IAS and the IAC and other assurance providers (external auditors, European Ombudsman);</li> <li>○ Prepare Europol's formal and informal response to the audit opinion of the ECA to the European Parliament (EP) on the annual accounts and to the discharge questionnaires by the EP;</li> <li>○ Maintain Europol's ethics package;</li> <li>○ Implement the Internal Control Framework, including the maintenance of the financial model of Europol (appointment decisions, etc.);</li> <li>○ Monitor the Internal Control System based on a dedicated list of internal control indicators with a view to assessing its effectiveness;</li> <li>○ Monitor Europol's corporate risks through the Corporate Risk Log for Europol, for assessment at Directorate level, carry out ad-hoc risk mitigation measures at the request of the Directorate.</li> </ul>
<p><b>Corporate communications</b></p>
<p><i>Manage open sources</i></p> <ul style="list-style-type: none"> <li>○ Provide access to, user support and training on the use of Open Source tools and databases. Organise the Europol Open Sources Intelligence Conference;</li> <li>○ Manage European Media Monitoring tool; deliver effective media monitoring, crisis monitoring and media impact products and services;</li> <li>○ Manage digital subscriptions and periodicals.</li> </ul>
<p><i>Internal communication</i></p> <ul style="list-style-type: none"> <li>○ Maintain and develop Europol's intranet as the main internal communication tool;</li> <li>○ Organise staff and managerial events.</li> </ul>
<p><i>Public relations</i></p> <ul style="list-style-type: none"> <li>○ Maintain media, press and public relations;</li> <li>○ Deliver annual and ad hoc media impact reports after events or operations;</li> <li>○ Support high level visits and organise high level events such as the European Police Chiefs Convention (EPCC);</li> <li>○ Coordinate external publications;</li> <li>○ Provide corporate audio-visual productions;</li> <li>○ Organise awareness-raising activities in Member States and Third Countries;</li> <li>○ Organise media training for Europol staff and annual photo competition.</li> </ul>
<p><b>Corporate services</b></p>
<p><i>Coordinate Europol participation in MB, MB Working Groups and follow up to MB decisions.</i></p>
<p><i>Corporate planning, monitoring and reporting</i></p> <ul style="list-style-type: none"> <li>○ Prepare the Europol Strategy on particular intervals and related multi-annual business planning documents;</li> <li>○ Prepare the annual business planning documents;</li> <li>○ Prepare quarterly, bi-annual and annual corporate performance reporting;</li> <li>○ Support and conduct internal and external stakeholder surveys and evaluations;</li> <li>○ Coordinate Europol's involvement in EU grant funded projects.</li> </ul>
<p><i>Corporate content management</i></p> <ul style="list-style-type: none"> <li>○ Coordinate corporate document and records management incl. archiving;</li> <li>○ Provide end user support and training for information management systems and services;</li> <li>○ Deliver process analysis, improvement and facilitation services;</li> <li>○ Ensure that all processes and protocols for new initiatives are in place to guarantee the methodological consistency of the work;</li> <li>○ Deliver training on quality and process management.</li> </ul>

## Europol Public Information

<p><i>Legal services – Commercial law</i></p> <ul style="list-style-type: none"> <li>○ Develop and maintain Europol’s legal framework for finance, procurement, grants and facilities;</li> <li>○ Advise on existing contract interpretation and escalation;</li> <li>○ Advise on litigation arising out of tender procedures and/or contracts;</li> <li>○ Review Europol’s participation in grant funded projects and awarding of grants;</li> <li>○ Handle contract related complaints to the European Ombudsman;</li> <li>○ Deliver internal training on legal procurement, low value contracts, contract management and legal issues in evaluation of tenders.</li> </ul>
<p><i>Legal services – Employment law</i></p> <ul style="list-style-type: none"> <li>○ Develop and maintain HR legal framework and implementing rules to the EU Staff Regulations;</li> <li>○ Provide legal advice concerning staff and HR related questions;</li> <li>○ Handle staff related complaints and requests including court cases to the European Ombudsman and the Court of Justice of the EU;</li> <li>○ Participate in lawyers' networks (EU IALN and international networks) and perform assessments following requests by IALN.</li> </ul>
<p><b>Procurement</b></p> <ul style="list-style-type: none"> <li>○ Coordinate tender planning in line with annual business and budget planning;</li> <li>○ Manage and supervise tender procedures;</li> <li>○ Continuously update procurement related implementing rules, policies, guidelines, documents, tender processes, tender model documentation, etc.;</li> <li>○ Deliver internal training on tenders;</li> <li>○ Participate in Network Agencies Procurement (NAPO) and exchange best practices on contract database and contract management.</li> </ul>
<p><b>Security</b></p> <p><i>Physical Security</i></p> <ul style="list-style-type: none"> <li>○ Ensure security of Europol staff, building and installations in compliance with European standards on operational security;</li> <li>○ Maintain close cooperation with relevant networks and other agencies; take part in peer reviews; attend conferences/ masterclasses on Safety &amp; Security;</li> <li>○ Provide training for security officers;</li> <li>○ Provide internal first aid, emergency response and evacuation training for staff;</li> <li>○ Deliver risk assessments related to Europol and its staff (e.g. for business trips).</li> </ul> <p><i>Confidentiality &amp; Information Security</i></p> <ul style="list-style-type: none"> <li>○ Ensure timely accreditation of information systems;</li> <li>○ Perform regular risk assessment of systems prior to becoming operational as well as compliance audits;</li> <li>○ Organise security awareness events and training for staff;</li> <li>○ Update information security policies;</li> <li>○ Regularly report to the Security Coordinator and the Security Committee;</li> <li>○ Handle requests for handling higher classified information;</li> <li>○ Handle clearance requests;</li> <li>○ Participate in EU security networks, international security forums or meetings organised by the Council Security Office.</li> </ul> <p><i>Internal Investigation Service</i></p> <ul style="list-style-type: none"> <li>○ Participate in the pool of internal investigators (as required by the Commission);</li> <li>○ Implement the Europol Anti-Fraud Strategy.</li> </ul> <p><i>Security Engineering</i></p> <ul style="list-style-type: none"> <li>○ Provide on-call assistance for technical security installations;</li> <li>○ Adjust, finalise and implement all technical security installations;</li> <li>○ Implement changes of security requirements in infrastructure.</li> </ul>

**Europol Public Information**

<p><i>Business Continuity</i></p> <ul style="list-style-type: none"> <li>○ Analyse, design, develop and implement the business continuity framework;</li> <li>○ Coordinate Europol's overall crisis management capability incl. organising an annual crisis management exercise for the Crisis Management Team;</li> <li>○ Coordinate Disaster Recovery activities.</li> </ul>
<p><i>Personal Protection</i></p> <ul style="list-style-type: none"> <li>○ Execute protective security operations for the Executive Director and staff;</li> <li>○ Coordinate and provide security in high level meetings and media events;</li> <li>○ Transport classified documents;</li> <li>○ Maintain tactical personal protection equipment and related security installations;</li> <li>○ Participate in the relevant European networks related to protection of public figures, personal protection services and threat assessment; support the related EPE.</li> </ul>
<p><b>Administration</b></p>
<p><i>Resource planning and reporting</i></p> <ul style="list-style-type: none"> <li>○ Establishment of the budget and staff establishment plan;</li> <li>○ Monitor the implementation of the budget and the staff establishment plan at corporate level;</li> <li>○ Report on Europol's financial and human resources to different stakeholders;</li> <li>○ Monitor activity based management;</li> <li>○ Manage the Financial Management System (ABAC).</li> </ul>
<p><i>Human Resource Management</i></p> <ul style="list-style-type: none"> <li>○ Develop and update HR related strategy, implementing rules, policies, guidelines, processes and templates;</li> <li>○ Organise the recruitment and selection of staff and SNEs; Follow up internal mobility;</li> <li>○ Plan and administer internships;</li> <li>○ Provide administrative support to Guest Officer deployments and to operational grants;</li> <li>○ Manage staff contracts and personal files;</li> <li>○ Manage ECAS accounts;</li> <li>○ Determine rights and entitlements of Europol staff, local staff and SNE's;</li> <li>○ Manage the salary administration;</li> <li>○ Administer working conditions and working hours of staff, as well as annual, medical and special leave;</li> <li>○ Ensure the HR-related relation with the Host State, including the administration related to the Protocol on Privileges and Immunities for Europol staff and ELO's;</li> <li>○ Represent Europol in the Advisory Board of the European School;</li> <li>○ Deliver health and wellbeing-related services;</li> <li>○ Implement actions in view of creating a corporate culture of diversity;</li> <li>○ Organise pre-employment and annual medical checks;</li> <li>○ Coordinate training of staff;</li> <li>○ Coordinate the appraisal and reclassification processes;</li> <li>○ Deliver pension advice;</li> <li>○ Manage the HR Management System and the Travel Management System.</li> </ul>
<p><i>Budget administration</i></p> <ul style="list-style-type: none"> <li>○ Develop and update finance related strategy, implementing rules, policies, guidelines, processes and templates;</li> <li>○ Execute financial initiation of revenue and expenditure;</li> <li>○ Perform ex-ante and ex-post financial verification of all financial operations;</li> <li>○ Manage the travel budget and refund of taxes.</li> </ul>
<p><i>Facilities Management</i></p> <ul style="list-style-type: none"> <li>○ Develop and update facilities-related strategy, implementing rules, policies, guidelines, processes and templates;</li> </ul>

## Europol Public Information

<ul style="list-style-type: none"> <li>○ Manage the facilities-related budget;</li> <li>○ Manage facilities-related contracts including the building insurance contracts;</li> <li>○ Manage the building(s), including housing, lease and service level agreements with the Host State as well as building related programmes;</li> <li>○ Manage the sites abroad, inclusive service level agreements, with the involved agencies and governmental institutes;</li> <li>○ Manage the non-ICT assets;</li> <li>○ Ensure an efficient space allocation in the building(s);</li> <li>○ Deliver meeting and conference services;</li> <li>○ Deliver travel management services;</li> <li>○ Coordinate translations with the Translation Centre For the Bodies of the EU (CdT);</li> <li>○ Manage and improve the Facilities Management Information System, Online Registration Tool and Conference Booking Tool.</li> </ul>
<b>ICT administrative support</b>
<p><i>Infrastructure Services</i></p> <ul style="list-style-type: none"> <li>○ IT Operations Centre: support and monitor all Europol IT Applications and Infrastructure;</li> <li>○ Define and maintain the technical profile and resource list;</li> <li>○ Periodically assess the need for profiles and technical skills;</li> <li>○ Run and maintain all non-ICT aspects of the Europol Datacentres.</li> </ul>
<p><i>Customer Service Centre</i></p> <ul style="list-style-type: none"> <li>○ Deliver Helpdesk services to external customers (MS and partners) and staff;</li> <li>○ Define and implement the request management process to handle all incoming requests from both customers and staff;</li> <li>○ Define and maintain MoU's for MS and partners.</li> </ul>
<p><i>Workplace Services</i></p> <ul style="list-style-type: none"> <li>○ Order, deploy and maintain end-user hardware and software;</li> <li>○ Periodic and urgent software and operating system patching of user-related hardware.</li> </ul>
<p><i>ICT Financial &amp; Contract Coordination</i></p> <ul style="list-style-type: none"> <li>○ Integrated ICT planning, financial management and financial administration;</li> <li>○ Supplier, license and asset management;</li> <li>○ Tender and procurement planning for ICT;</li> <li>○ ICT contract management.</li> </ul>

## 2019 Objectives

A.7.1. Continue optimising Europol's corporate functions.	
Actions	<p>Establish the new Europol Financial Regulation in line with the new Framework Financial Regulation and update model contracts accordingly.</p> <p>Ensure that all processes and protocols for new initiatives are in place to guarantee the methodological consistency of the work.</p> <p>Develop an Analytics and Reporting capability to ensure high-quality and accurate corporate performance measurement and reporting.*</p> <p>Implement corporate risk and audit management tooling for cross-organisational use.</p>

## Europol Public Information

---

Adjust HR policies according to the requirements of the TA 2(f) article of the Staff Regulation.

Procure and implement ICT capabilities for electronic management of documents and records. Progress in establishing ICT capabilities that enable electronic workflows and electronic approval. Further digitalise processes in HR financial and facilities management. Implement e-recruitment for restricted posts.

Fully utilise the e-submission module for all applicable procurement procedures. Continue introducing pre- and post-awarding e-procurement solutions (subject to release of e-PRIOR modules by the Commission).

Implement the basic modules of the HR management system (Sysper2).

Assess the feasibility of implementing the Missions Integrated Processing System (MIPS) as the new travel management system at Europol.

Progress with aligning Europol's archiving of official documents with EU Archive Regulation 2015/496 amending Council Reg 354/1983.

Streamline the processing of the increasing number of requests for public access to Europol's documents.

Continue the setting up of an environmental management system complying with ISO 14001 requirements and the EU Eco-Management and Audit Scheme (EMAS) to improve the sustainability environmental awareness and resource efficiency of the organisation. Start the EMAS registration process with the national competent body.

Ensure efficient coordination of the provision of in-house training coordination for Europol's staff.

Conduct the biennial Staff Engagement Survey.

Conclude a Service Level Agreement with the EEAS for provision of security services to travelling Europol's staff.

Initiate a revision and insourcing of Europol's medical service.

Explore the possibility to expand the technical capacity for teleworking.

Continue with the screening of job descriptions in order to further align job positions and entry grades for Europol's staff.

Continue expanding the shared services with other EU agencies and in particular with Eurojust.

---

Expected results

Up-to-date policies and processes and reduced administrative burdens.

Bureaucracy and time spent on document and records management and reporting are reduced while ensuring the availability of reliable information on decision making, corporate performance and level of compliance.



## Europol Public Information

Increased HR efficiency, effectiveness and customer service delivery.

### A.7.2. Progress towards the rationalisation and expansion of Europol's capabilities in order to accommodate the growth of the agency.

Actions	<p>In collaboration with the Host State, complete the necessary procedures to set up the temporary satellite building and ensure the smooth transfer of staff. Explore the possible expansion to a second temporary satellite building, if needed.</p> <p>Following the outcome of the floor surface risk audit, ensure that remedial actions are taken under the responsibility of the Host State. Continue the planning activities to maximise the efficient usage of Europol's headquarters building.</p> <p>Deliver the functional and technical requirements and tender the design for a new additional permanent building to provide for a long term housing solution.</p> <p>Fulfil all the requirements in terms of procurement, logistics, ICT and security for the establishment of the new Decryption platform capacities at the JRC premises in Italy.</p> <p>Finalise the upgrade of the audio-video installation in the conference environment.</p> <p>Evaluate whether existing plans and procedures (e.g. Europol's Crisis Management Plan) are still fit-for-purpose vis-à-vis the new building developments and identify areas for further improvement/adjustment.</p> <p>Finalise the setting up of the new ICT delivery model - Software factory - allowing for increased capacity to handle growing demand for ICT services while ensuring compliance with quality and security standards.</p> <p>Revise the ICT Disaster Recovery approach while assessing the risk and the need for re-architecture and more efficient resource utilisation, and by exploring possibilities to introduce novel techniques.</p>
---------	---

Expected results	<p>Existing workspace and new office locations are used in an optimal way to accommodate organisational growth.</p> <p>Europol is better equipped to handle increasing demand for ICT services.</p>
------------------	---

### A.7.3. Establish a new strategy <sup>25</sup> for effective awareness raising on Europol's products and services to law enforcement stakeholders.

Actions	<p>Organise a workshop with internal communicators of the MS competent authorities in order to identify the best way forward regarding the different available communication tools (e.g. Intranet, e-learning, webinars, etc.).</p> <p>Organise consultation with trainers of the police academies of MS competent authorities to identify possibilities to</p>
---------	---

<sup>25</sup> Provisional name until the document is finalised and agreed in 2019.

**Europol Public Information**

	<p>include Europol's remit services and tools in the training curriculum for junior police officers. Decide on modalities on how to implement a Train-the-Trainers concept in order to have a pool of trainers in MS who are knowledgeable about Europol's products and services.</p> <p>Liaise with the Heads of the Liaison Bureaux and exchange/discuss ideas regarding the joint approach to raise awareness of international cooperation.</p> <p>Approach CEPOL with regards to establishing synergies with CEPOL's webinar programme.</p>
Expected results	A consolidated awareness raising strategy is agreed with MS's law enforcement stakeholders.

(\* The level of implementation of actions marked with an asterisk throughout the Work Programme depends on the availability of additional resources.)

Indicators	Latest result Q3 2018	Target 2019
Administrative ICT project and work packages delivery (% of milestone points achieved)	-	75%
Uptime of administrative systems	98.6%	98%
<i>Commitment Rate Europol Budget</i>	84.7%	≥ 95%
<i>Payment Rate Europol Budget</i>	62.7%	≥ 90%
Budget Outturn rate	-	≤ 2%
% Late Payments	13%	≤ 5%
<i>Vacancy rate</i>	3.6%	≤ 2%
<i>Sickness rate</i>	-	≤ 3.5%
Turnover rate	4.5%	10%
<i>% of pending critical/very important audit recommendations implemented within the agreed deadline with the auditing body</i>	71%	85%
% of Work Programme objectives implementation	-	80%
% Staff Engagement (via Staff Survey)	-	65%
<i>% Satisfaction with Europol's image (via User Survey)</i>	-	79%
Number of Europol's appearances in the media	82,509	130,000

## Management Board Functions

### Accountancy Unit (ACCU)

The Accountancy Unit is an independent unit within Europol with its Accounting Officer appointed by/reportable directly to Europol's Management Board (MB). Its main tasks and responsibilities are to:

- Implement all payments (including salaries and allowances);
- Collect revenue and recovering amounts established as being receivable;
- Implement the accounting rules and chart of accounts in accordance with the provisions adopted by the European Commission;
- Keep, prepare and present the annual accounts of Europol (financial statements and reports on the implementation of the budget);
- Lay down and validating the accounting systems; Manage the Treasury.

### Data Protection Function (DPF)

The DPF is an integral part of Europol and the initial point of contact for all data protection matters. The Data Protection Officer who acts as the Head of DPF is appointed by the MB in accordance with Article 41 ER. DPF main tasks and responsibilities are to:

- Ensure lawfulness and compliance in regards to data protection (e.g. compliance reviews, annual activity report, written record of the transmission of data, register of processing operations, handling of data subject request, handling of inquiries etc.);
- Provide consultation in relation to legal and technical-organisational data protection safeguards;
- Provide training and awareness program for staff handling personal data;
- Perform as the main contact point to external data protection supervisors (e.g. Europol Data Protection Supervisor / National Data Protection Authorities).

### Internal Audit Capability (IAC)

With the entry into force of the Europol Regulation, the IAC was formally established and continued the work of the Internal Audit Function with the mission to enhance and protect Europol's organisational value, by providing risk-based and objective assurance, advice and insight. Its main tasks and responsibilities are to:

- Evaluate the appropriateness of Europol's risk identification and management system, and the effectiveness of the Internal Control Framework (ICF);
- Review the arrangements established to ensure compliance with applicable legislation, policies, plans and procedures;
- Review the reliability and integrity of significant operating and financial information and the means used to identify, measure, classify and report such information;
- Evaluate the economy and efficiency with which resources are employed;
- Review programs or operations to ascertain whether results are consistent with established plans and objectives, and determine whether goals have been achieved;
- Monitor and report on the implementation of audit recommendations issued by IAC.

### Management Board Secretariat (MBS)

MBS is responsible for supporting the Chairperson of the Management Board in compliance with the Europol Regulation. Its main tasks and responsibilities are to:

- Support the coordination of the MB's work and ensure its coherence;
- Organise activities and meetings of the MB and its Working Groups on Corporate matters (legal, financial and personnel issues) and on ICT, as well as ad hoc meetings and working groups established by the Board;
- Provide the MB with the administrative support;
- Support oversight and policy-making activities regarding matters such as the appointment of Executive Directors and Deputy Executive Directors, corporate governance, human resources and external relations.