The Hague, 29 January 2019
EDOC#   924131v19

Europol Programming Document

2019 – 2021

Adopted by Europol Management Board on 30.11.2018[1]

---

[1] Section II.3 and Annexes I-III and IX-X updated after adoption of the Union budget 2019 and upon availability of 2018 final end of year figures.

Table of Contents

List of Acronyms

ADEP	Automation of Data Exchange Processes
AP	Analysis Project
ARO	Asset Recovery Office
BPL	Basic Protection Level
CBRN	Chemical, Biological, Radiological and Nuclear
CEPOL	European Union Agency for Law Enforcement Training
COSI	Standing Committee on Operational Cooperation on Internal Security
CSDP	Common Security and Defence Policy
CT	Counter-Terrorism
DPF	Data Protection Function
EC3	Europol Cybercrime Centre
ECA	European Court of Auditors
ECTC	European Counter Terrorism Centre
EEAS	European External Action Service
EES	Entry-Exit System
EIS	Europol Information System
EMAS	Europol Malware Analysis Solution
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMPACT	European Multidisciplinary Platform against Criminal Threats
EMSC	European Migrant Smuggling Centre
EPE	Europol Platform for Experts
ESOCC	European Serious and Organised Crime Centre
ETIAS	EU Travel Information and Authorisation System
ETS	European Tracking Solution
EUIPO	European Union Intellectual Property Office
Eurojust	The European Union's Judicial Cooperation Unit
EU RTF	EU Regional Task Force
Eu-Lisa	European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice
FIU	Financial Intelligence Unit
Frontex	European Border and Coast Guard Agency

HR	Human Resource
HVT	High Value Targets
IAC	Internal Audit Capability
IAS	Internal Audit Service
ICT	Information and Communications Technology
IDMC	Integrated Data Management Concept
IRU	Internet Referral Unit
ISF	Internal Security Fund
J-CAT	Joint Cybercrime Action Taskforce
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
JOT	Joint Operation Team
JRC	Joint Research Centre
LEA	Law Enforcement Authorities
MB	Management Board
MENA	Middle East and North Africa region
MS	Member State
MTIC	Excise and Missing Trader Intra Community
OAP	Operational Action Plan (under EMPACT)
OCG	Organised Crime Group
OLAF	European Anti-Fraud Office
OSINT	Open Source Intelligence
OSP	Online Service Providers
PIU	Passenger Information Unit
PNR	Passenger Name Record
QUEST	Querying Europol's systems
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
SOC	Serious and Organized Crime
SOCTA	Serious and Organized Crime Threat Assessment
TFTP	Terrorist Finance Tracking Programme
THB	Trafficking in human beings
TP	Third Parties
UMF	Universal Message Format
VIS	Visa Information System

Mission Statement

Europol's mission is to support its Member States in preventing and combating all forms of serious international and organised crime and terrorism.

SECTION I – General Context

This section presents policy factors that are expected to influence Europol's work in the coming years.

1. Security Union

1.1. European Agenda on Security

Europol's work directly contributes to the European Agenda on Security 2015 - 2020 on each of the three priorities identified: Terrorism and Radicalisation, Serious and Organised Crime, and Cyber Crime.

In addition to these priorities, Europol actively participates in the inter-agency and cross-sectorial approach against security threats promoted by the Agenda, and aims at strengthened cooperation with neighbouring countries, strengthened cooperation with the private sector to fight online crime and better law enforcement information exchange across the EU.

Finally, Europol continues to support the EU Policy Cycle for serious and organised crime and promotes the use of Joint Investigation Teams (JITs). The embedment of FIU.NET in Europol contributes to cross-border cooperation between national Financial Intelligence Units (FIUs) and national Asset Recovery Offices (AROs), ensuring operational cooperation to combat money laundering and to access the illicit proceeds of crime.

1.2. European Commission's 2018 Security Package

On 17 April 2018, the Commission adopted a set of new security proposals to further reduce the space in which terrorists and criminals operate - denying them the means to plan, finance and commit crimes. The package includes five proposals, relevant to Europol's work:

- **Document fraud**: Proposal for a regulation on strengthening the security of identity cards and residence documents of Union citizens.
- **Financial information**: Proposal of a Directive aiming at facilitating the use of financial information in criminal matters. The proposal complements and extends the 5th Anti-Money Laundering directive.
- **Explosives precursors**: Proposal of a regulation to further restrict access to dangerous substances by banning two new explosives precursors and strengthening the existing rules for both online and offline sales.
- **Export and import of firearms**: the Commission updated EU rules on the export and import of civilian firearms to include improved control procedures and enhanced information exchange and issued a recommendation on immediate steps to improve the security of export, import and transit measures for firearms, their parts and essential components and ammunition.
- **E-evidence:** Proposal for a new legislation on electronic evidence (see section below: cybercrime).

1.3. European Commission's Western Balkans Strategy

On 2 February 2018, the European Commission adopted a communication on "A credible enlargement perspective for and enhanced EU engagement with the Western Balkans" (Western Balkans Strategy), which foresees reinforced engagement of Europol with Western Balkan countries on security and migration. Specifically, the Communication foresees the deployment of Europol Liaison Officers to the region and the further promotion of Joint Investigation Teams. Following this communication, Europol signed a grant agreement with the Commission in February 2018 for the implementation of a pilot deployment to three

selected Western Balkan countries (Albania, Bosnia and Herzegovina, and Serbia) for 18 months. The first deployments are foreseen in 2019.

1.4. Strengthening cooperation with CSDP missions and operations

The European Council conclusions of 19 October 2017 called for enhanced information exchange between JHA Agencies and CSDP missions and operations. Furthermore, the Council conclusions on strengthening civilian CSDP of 28 May 2018 called for increased coherence and cooperation between civilian CSDP and actions undertaken by the EU in the external dimension of Justice and Home Affairs, as well as for fostering synergies between the CSDP and JHA actors on the operational level to increase information exchange. Europol considers civilian CSDP missions and operations as useful means to gather criminal information and to facilitate contacts with local authorities and views positively an early consultation of JHA actors in the planning phase of CSDP missions.

2. <u>Serious and Organised Crime</u>

2.1. European Public Prosecutor's Office (EPPO)

Regulation (EU) 2017/1939 establishing the European Public Prosecutor's Office entered into force in November 2017. The office should be fully established by end-2020 and Europol is required to assist the office in its mission to investigate and prosecute criminal offences affecting the financial interests of the Union.

3. <u>Migration</u>

3.1. European Agenda on Migration

The European Agenda on Migration came into life in May 2015 and led to the creation of the European Migrant Smuggling Centre (EMSC) at Europol. A number of measures emerged in the context of the Agenda, with Europol strengthening its cooperation with Frontex, Eurojust and EASO through the hotspot approach and other specific tasks defined in the Agenda. In addition, Europol was tasked with identifying illegal online content used by smugglers to attract migrants and refugees, and with requesting its removal.

The Agenda on Migration stipulates that EU Agencies can also assist Member States' authorities in conducting proactive financial investigations, aiming at seizures and recovery of criminal assets, and actions against money laundering connected to migrant smuggling which can be supported through enhanced cooperation with FIUs on financial flows and new cooperation with financial institutions, such as banks, international money transfer services, and credit card issuers. Cooperation with third countries is also of critical importance.

3.2. Malta Declaration on the external aspects of migration

The Malta Declaration on the external aspects of migration (2017) and the subsequent Implementation Plan re-confirmed and escalated further the role of the European Migrant Smuggling Centre at Europol in supporting EU MS to tackle migrant smuggling and trafficking in human beings. In particular, the EMSC is expected to collect, analyse and disseminate evidence and intelligence from/to all relevant actors, with a view to closing intelligence gaps, providing a common risk analysis and assessment, and identifying investigative opportunities. Closer cooperation with EU bodies (including missions/operations and EU delegations) and the posting of Europol liaison officers to key partners for the stimulation of enhanced information exchanges should assist this process.

3.3. European Council Conclusions June 2018

In June 2018, the European Council introduced the concept of "regional disembarkation platforms" to be established on third countries' territory in cooperation with the relevant countries, the UNHCR and the IOM. In addition, the Council proposed to establish "controlled centres" on EU territory for a rapid and secure processing of asylum requests and the subsequent repatriation, relocation or resettlement. The Commission further elaborated these concepts by issuing two non-papers in July 2018, foreseeing a specific role for Europol to conduct security checks in the controlled centres.

4. <u>Terrorism and radicalization</u>

4.1. European Commission's Counter-Terrorism package (October 2017)

In 2017 the Commission presented a set of operational and practical measures to better defend EU citizens against terrorist threats. The Commission proposed, in addition, to further strengthen the EU's external action on counter-terrorism by enhancing Europol's cooperation with third countries. Subsequently, the Commission presented recommendations to the Council who authorised the opening of negotiations for agreements between the EU and Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey on the transfer of personal data between Europol and these countries in order to prevent and combat terrorism and serious crimes. The conclusion of the agreements is expected to progress over a number of years.

Finally, the Commission proposed an Action Plan to step up EU level preparedness, resilience and coordination against attacks involving chemical, biological, radiological and nuclear (CBRN) substances, including the creation of an EU CBRN security network and a CBRN knowledge hub to be set up in the European Counter-Terrorism Centre at Europol.

4.2. European Commission's Communication and Recommendation on tackling illegal content online

The availability and proliferation of illegal content online remain an important public policy and security concern in the EU. The Commission responded to the challenge in a variety of ways, through the Communication on Tackling Illegal Content Online (2017) and, more recently, through the Recommendation on Measures to effectively tackle illegal content online (March 2018). In particular, the Commission recommends that:

- MS should ensure that their competent authorities have the capability and sufficient resources to effectively detect and identify terrorist content and to submit referrals to the hosting service providers concerned, in particular through national internet referral units and in cooperation with the EU Internet Referral Unit (EU IRU) at Europol;
- Provision should be made for mechanisms allowing for the submission of referrals. Fast-track procedures should be provided to process referrals, in particular referrals submitted by national internet referral units and by the EU IRU;
- Hosting service providers should, without undue delay, send confirmations of receipt of referrals and inform the competent authority or Europol of their decisions with respect to the content to which the referrals relate, indicating, as the case may be, when the content was removed or access thereto was disabled or why they decided not to remove or to disable access to the content.
- Hosting service providers should assess and, where appropriate, remove or disable access to content identified in referrals, as a general rule, within one hour from the moment at which they received the referral.

4.3. Foreign Affairs Council Conclusions on the EU External Action on Counter-terrorism

On 19 June 2017, the Foreign Affairs Council adopted conclusions on the EU external action against terrorism, welcoming the revised Europol mandate as means to contribute more effectively to the fight against terrorism and to ensure greater coherence between internal and external actions in the field of security. In addition, the Council noted the importance of supporting cross-border investigations and prosecutions of foreign terrorist fighters and encouraged further engagement in this area through Europol law enforcement cooperation with priority countries. The Council also called on continued assessment of the link between serious and transnational organised crime and terrorism.

4.4. High-level Commission Expert Group on Radicalisation (HLCEG-R)

The HLCEG-R adopted its final report in May 2018. It identifies a number of priority areas, including the countering of online propaganda, the need to support first-line practitioners at local level in a multi-agency setting, and the importance of information exchange on

radicalised persons and radicalisation pathways. Moreover, the report acknowledges the nexus between internal and external security and supports closer engagement with third countries and international organisations. The Expert Group also proposed setting up an EU Cooperation Mechanism to connect the main stakeholders in the field of prevention of radicalisation.

4.5. European Parliament's Recommendation on terrorist financing

In March 2018, the European Parliament (EP) approved a recommendation on cutting the sources of income for jihadists – targeting the financing of terrorism. The EP called on MS to improve coordination and cooperation by setting up a stable European counter-terrorism financial intelligence platform, within the framework of existing structures (e.g. Europol) as to avoid the creation of another agency, with an in-depth focus on the proactive exchange of information on the financial support for terrorist networks; recommended the introduction of quarterly public threat assessments that combine the intelligence and information gathered by Europol and INTCEN; called for cooperation between Europol and the EU's key strategic partners that play a crucial role in the fight against terrorism worldwide to be reinforced; called on the MS to make better use of the FIU.net, on the basis of the work done by Europol; called on the MS to step up the monitoring of suspicious organisations engaged in these kind of activities via the establishment of joint investigation teams with Europol.

5. <u>Cybercrime</u>

5.1. European Commission's Cyber policy package of 15 September 2017

In September 2017, the Commission adopted a new package on cybersecurity with a wide-ranging set of measures to reinforce the EU's resilience and response to cyber-attacks. The package comprises several elements that are of direct relevance to Europol, as outlined in the Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" [2], the proposal for a Directive on Non-Cash Payment Fraud [3] and the Recommendation "on Coordinated Response to Large Scale Cybersecurity Incidents and Crises"[4].

5.2. European Commission's e-evidence package

In April 2018, the Commission proposed a legislative package aiming at facilitating and accelerating law enforcement and judicial cross-border access to electronic evidence (data stored in an electronic format that is relevant in criminal proceedings). More and more such data is stored by service providers in the cloud, on servers in third countries, or with providers outside the EU, and hence it is difficult to obtain for law enforcement and the judiciary. The objective of the package is to establish a consistent legal framework and avoid conflicting obligations with the law of non-EU countries, as well as to protect the fundamental rights of individuals.

Conceived as a judicial cooperation tool, the e-evidence legislation could have implications for Europol, since the SIRIUS capability is mentioned in the Draft Regulation as a possible platform to transmit and facilitate the authentication of orders and as a de-confliction tool.

6. <u>Information exchange and interoperability</u>

6.1. Regulation establishing a framework for interoperability

The work on the interoperability of information systems started with the roadmap on information exchange [5] endorsed by the Justice and Home Affairs Council in 2016 and continued with the high-level expert group on information systems and interoperability,

---

[2] JOIN(2017) 450 final
[3] Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (COM(2017) 489 final)
[4] Commission Recommendation of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (C(2017) 6100 final)
[5] Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area, 6 June 2016, Council Secretariat file no. 9368/1/16

which issued its final report[6] in 2017 with a set of findings and recommendations. On 12 December 2017, the Commission tabled two sister proposals to establish a framework for interoperability between existing and future EU information systems for police and judicial cooperation, asylum and migration – namely the EES, the VIS, ETIAS, Eurodac, the SIS and the ECRIS-TCN – in order for those systems and data to supplement each other.

The new regulation will establish:

- A common identity repository (CIR). The CIR would allow for the creation of an individual file for each person that is recorded in the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN.
- The European search portal (ESP) to enable the simultaneous querying of the EES, the VIS, the ETIAS, Eurodac, the SIS, the ECRIS-TCN as well as of Europol data and the Interpol databases.
- A shared biometric matching service (shared BMS).
- A multiple-identity detector (MID).
- A new framework for MS law enforcement authorities' and for Europol' access to the EES, the VIS, ETIAS and Eurodac provided by the CIR.

6.2. Recast of Eurodac Regulation

The proposal to recast the Eurodac Regulation would extend the use of Eurodac to the purpose of identifying illegally staying third-country nationals in the EU and those who have entered the EU irregularly at the external borders, with a view to using this information to assist MS for return purposes.

6.3. European Commission's proposal to improve and extend the use of SIS

The Commission proposed in December 2016 a set of three proposals to improve and extend the use of SIS, in accordance with the objective of improving interoperability between EU information systems. The proposal would, among others:

- Create a new alert category for "unknown wanted persons" with full access rights for Europol;
- Introduce the obligation to create SIS alerts in cases related to terrorist offences;
- Extend Europol's access rights to SIS alerts on missing persons to improve the agency's support to law enforcement authorities in cases concerning trafficking in human beings and child sexual exploitation;
- Ensure that MS share information on terrorism and foreign terrorist fighters with Europol in parallel to introducing alerts in SIS, in order to allow ECTC to cross-check the information with Europol's databases and to provide analysis;
- Grant EMSC access to alerts on persons who are refused entry or stay within the territory of a MS either on criminal grounds or because of non-compliance with visa and stay conditions.

6.4. Recast of the Visa Information System

In May 2018, the Commission proposed a new regulation to upgrade and extend the use of VIS. The proposed regulation foresees a more structured access to VIS for Europol and other MS' law enforcement authorities, in full respect of EU rules on data protection. As specifically mentioned in the draft legislation, Europol would be entitled to receive about €30 million between 2021 and 2027 for the development of an ABIS (Automated Biometrics Identification System) necessary to cross-check fingerprints/facial images included in VIS against Europol's biometric data.

6.5. European Travel Authorization System (ETIAS)

In 2016, the Commission proposed the establishment of ETIAS which would allow visa-exempt third country nationals to obtain a travel authorisation prior to their travel to the Schengen Area, via an online application. The data provided by applicants will be cross-checked, amongst others, against Europol's database. ETIAS will be managed by Frontex in

---

[6] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

close cooperation with the competent authorities of the MS and Europol. Europol will be able to request consultation of data stored in the ETIAS Central System to support MS in investigating criminal offences falling under its mandate and may be consulted by ETIAS National Units in the follow-up to a hit. Europol will also be tasked with managing a dedicated ETIAS Watch List.

ETIAS is expected to be fully operational by 2021.

6.6. Entry-Exit System (EES)

The new Entry/Exit System should replace the stamping of passports and apply to all non-EU nationals who are admitted for a short stay into the Schengen area. Expected to be operational in 2020, the system's objective is to facilitate the border crossing of good faith travellers, detect over-stayers and support the identification of undocumented persons in the Schengen area.

Europol would be able to request access to the EES, under specific authorisation and data protection rules.

6.7. Implementation of the PNR Directive

The PNR Directive provides for the establishment or designation in MS of an authority competent for law enforcement to act as a Passenger Information Unit (PIU). PIUs are entitled to process PNR data and are responsible for the cross-border transfer of both PNR data and the result of its processing thereof to corresponding national PIUs and to Europol.

6.8. Europol Regulation – information exchange and management

The Europol Regulation (ER) entered into force on 1 May 2017. In addition to giving Europol a number of new tasks that are now integrated in the structure of the organisation, the ER provided the opportunity to introduce a new concept for Integrated Data Management which allows handling data based on the purpose of the processing. The new information management architecture is system-agnostic, flexible and operationally driven. In order to reap its full benefits, a multi-annual implementation plan will be required to adjust Europol's technological landscape.

The new ER also expands the possibilities regarding the cooperation of Europol with EU bodies, Third Parties and private partners.

7. <u>EU Policy Cycle for organised and serious crime 2018-2021</u>

The Council adopted in 2017, on the basis of Europol's SOCTA, **ten priorities** for the EU policy cycle for organised and serious international crime for the period 2018-2021, which largely determine the priority work of Europol for the coming years. The priorities are:

1) To fight cybercrime, by (1) disrupting the criminal activities related to attacks against information systems, particularly those following a Crime-as-a-Service business model and working as enablers for online crime, by (2) combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, and by (3) targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities.

2) To (1) disrupt the activities of Organised Crime Groups (OCGs) involved in the wholesale trafficking of cannabis, cocaine and heroin to the EU, to (2) tackle the criminal networks involved in the trafficking and distribution of multiple types of drugs on EU markets and to (3) reduce the production of synthetic drugs and New Psychoactive Substances (NPS) in the EU and to dismantle OCGs involved in their production, trafficking and distribution.

3) To disrupt OCGs which facilitate illegal immigration by providing facilitation services to irregular migrants along the main migratory routes crossing the external border of the EU and within the EU, particularly focussing on those whose methods endanger people's lives and those offering their services online, and making use of document fraud as part of their business model.

4) To combat organised property crime by concentrating on disrupting highly mobile OCGs carrying out organised thefts and burglaries across the EU. This should include OCGs using new technologies or enhanced countermeasures which exploit the lacking interoperability of cross-border surveillance tools.

5) To fight against the trafficking in human beings (THB) in the EU for all forms of exploitation, including sexual and labour exploitation as well as all forms of child trafficking.

6) To disrupt the capacity of OCGs and specialists involved in excise fraud and Missing Trader Intra Community (MTIC) fraud.

7) To disrupt OCGs involved in the illicit trafficking, distribution and use of firearms.

8) To disrupt OCGs involved in environmental crime, more specifically wildlife and illicit waste trafficking.

9) To combat criminal finances and money laundering and facilitate asset recovery in view of effectively confiscating the criminal profits of OCGs, especially targeting money laundering syndicates offering money laundering services to other OCGs and those OCGs making extensive use of emerging new payment methods to launder criminal proceeds.

10) To combat document fraud in the EU, by targeting OCGs involved in the production and provision of fraudulent and false documents to other criminals.

8. <u>Multiannual Financial Framework</u>

8.1. Multiannual Financial Framework 2014-2020

The MFF is a key consideration as it provides the financial and human resource ceilings for the implementation of Europol's multi-annual programming and annual objectives. Elaborated in 2013, the MFF provided for very limited growth of the agency, despite the establishment of entirely new tasks such as EC3. The growth of cybercrime, the migration crisis and terrorist threats of recent years have triggered some relevant adjustments to the provisions of the MFF, in particular in 2016 and 2017, when Europol received additional resources, to support priority areas of work.

In order to ensure that the full impact of new developments and tasks assigned to Europol are adequately reflected in the Union's budget, Europol assesses its resource needs on an annual basis and adjusts its level of ambition in terms of implementation of its Work Programme, to match the Budgetary Authority's decision.

8.2. Multiannual Financial Framework 2020+

The MFF 2020+ (2021-2027) is under development at the time of preparing this document. Based on the Commission's proposal (May 2018) for the new MFF, a general increase of funds dedicated to internal security is foreseen compared to the previous MFF. In line with the Commission's acknowledgment of the need to further strengthen EU Agencies in the field of security, including Europol, the financial and human resources programming for 2021 and 2022 is based on the assessment of Europol's needs.

SECTION II - Multi-annual programming 2019 – 2021

1. Multi-annual objectives

Based on the Financial Regulation and following Commission guidelines, Europol has prepared its Programming Document 2019-2021 containing multi-annual and annual programming components combined with indicative budget and resource allocations.

The multi-annual component of the Programming Document is largely based on the Europol Strategy 2016-2020 which was adopted by Europol's Management Board on 1 December 2015. The agreed strategic objectives are incorporated in the Programming Document as multi-annual objectives and are linked to the 2019 annual work programme, objectives and actions under Section III. At the time of writing, a mid-term review of the Europol Strategy is underway while the development of multi-annual strategic objectives covering the years 2020+ should take place in 2019.

Goals 2016-2020	Multi-annual objectives 2019-2021
Goal 1: Europol will be the EU criminal information hub, providing information sharing capabilities to law enforcement authorities in the MS	1.1. Develop the necessary ICT capabilities to maximise the exchange and availability of criminal information
	1.2. Provide effective and immediate first-line information exchange
	1.3. Strategically enhance partnerships with cooperation partners
Goal 2: Europol will provide the most effective operational support and expertise to MS investigations by developing and employing a comprehensive portfolio of services	2.1. Support MS investigations in the area of Serious and Organised Crime (SOC)
	2.2. Support MS investigations in the area of cybercrime
	2.3. Enhance cooperation in the area of counter-terrorism (CT)
	2.4. Develop and manage high quality analytical support and an evolving portfolio of cross-cutting operational capabilities
Goal 3: Europol will be an efficient organisation with effective governance arrangements and a positive reputation	3.1. Ensure effective, efficient and accountable management of Europol's resources
	3.2. Promote the added value and achievements of EU law enforcement cooperation to stakeholders and EU citizens

2. Multi-annual programme

Goal 1: Europol will be the EU criminal information hub, providing information sharing capabilities to law enforcement authorities in the MS

The information management capabilities of Europol lie at the heart of its mandate, as they allow for increased cooperation between the Member States and Europol, and are crucial in obtaining the necessary intelligence to tackle cross-border crime. Information management includes the access to, collection and organisation of the structure, processing and delivery of information from multiple sources and in multiple formats to the Member States. To achieve its goal, Europol's work will focus on three axes: firstly on designing and building the new information architecture of the organisation, in particular in the context of the integrated data management concept afforded by the Europol Regulation and in the context of improved EU interoperability of information systems; secondly, on the provision of fast, reliable and uninterrupted first line response and thirdly, on enhancing partnerships to develop a more comprehensive intelligence picture.

1.1 Develop the necessary ICT capabilities to maximise the exchange and availability of criminal information

Europol will exploit new technological developments and be a significant contributor to the increased integration and interoperability of law enforcement systems in Europe.

The new legal framework of Europol removes the emphasis from specific ICT systems and databases and introduces a new integrated data management concept (IDMC) which focuses, first and foremost, on placing the business needs of the law enforcement community as the main driver of obtaining, storing and disseminating the information available. In concrete terms, the rules for information processing are related to the data itself – rather than the systems or databases used to store it. As a consequence Europol, in close consultation with Member States, will have the opportunity to use this flexibility to modernise its systems architecture and information management strategy to ensure the best ways to manage criminal information and enhance the analytical capabilities of Europol based on MS' operational requirements. The integration of data will ensure that links across crime areas will be more easily identified and therefore, analytical support will be of increased value. The implementation of this new concept will lead to an evolution of existing systems such as the EIS and the development of new ICT solutions, including means of innovation such as, data science and 'smart' technologies.

Other major drivers behind information exchange capabilities will be the ever-increasing amount of available information and new technological trends such as de-centralised systems of information sharing. Europol will work towards providing Member States with optimal solutions by examining and applying the most appropriate topologies (e.g. central collecting or connecting data, ADEP concept) to ensure the necessary access to information and the provision of a complete intelligence picture. The access to and cross-checking of data in databases such as Prüm, SIS II and VIS will also be considerations of the new design. Travel intelligence such as PNR and ETIAS are expected to have a significant effect on the requirements of Europol's infrastructure.

Europol will build on the success of SIENA and further develop the Agency's messaging capability to remain the first choice for secure law enforcement information exchange and communication.

1.2. Provide effective and immediate first-line information exchange

The information intake and data handling model will be built in line with the new integrated data management concept, taking into account the increasing influx of high volume data.

Europol will respond to the needs of Member States for fast and uninterrupted service in a number of ways. A first-line 24/7 information hub is available to maximise intake, initial processing and availability of information to Member States. In addition, Europol will work

with Member States to increase the quality of their cooperation, in particular with regard to the quality of information exchanged and the speed of response (e.g. through increased usage of the Universal Message Format (UMF)).

Finally, Europol will further invest in standardisation, automation of cross-matching, optimisation of information flows and flexible resource allocation with a view to making more efficient use of human resources while managing to respond to all information processing requests in a timely manner.

1.3. Strategically enhance partnerships with cooperation partners

An enhanced multi-disciplinary approach is becoming increasingly more relevant for Europol in delivering its mission, bringing together necessary expertise and information from an expanding range of partners.

Europol will continue to promote and further develop its cooperation with all competent law enforcement authorities including Customs and Counter-Terrorism services in the MS. At the same time, Europol will aim to further strengthen its partnership with third states (e.g. US, Mediterranean countries, the Western Balkans, Middle East and North African countries), through initiatives which preserve Europol's operational nature and its support function to Member States. In view of the global challenges the EU is facing, for example in the area of cybercrime, migration and terrorism, cooperation with Interpol will remain particularly relevant and will be enhanced through closer alignment and setting of common strategic actions.

EU agencies (e.g. Frontex, Eurojust) will remain important partners and cooperation will be further enhanced on the basis of complementarity. In particular, Europol and Frontex will closely cooperate in matters related to irregular migration while Europol and Eurojust will continue strengthening their cooperation through Joint Investigation Teams and in the area of cybercrime. The work of Europol on Intellectual property crime will be enhanced through the cooperation with EUIPO. Cooperation with other agencies, especially in the area of Justice and Home Affairs (e.g. CEPOL, eu-LISA, FRA), is being developed and implemented as needed for initiatives of common interest.

In addition, and more significantly than in the past, Europol's ability to cooperate with the private sector will be key in achieving the best operational results; the provisions of the new Europol Regulation will largely determine the extent to which Europol will cooperate with private partners.

The new External Strategy 2017-2020 as endorsed by Europol's Management Board at the end of 2016 has further defined the focus and steps to be taken towards enhancing cooperation with third countries and international organisations (please see next chapter).

Goal 2: Europol will provide the most effective operational support and expertise to MS investigations by developing and employing a comprehensive portfolio of services

Europol will provide high quality operational support to MS investigations in three key priority areas, aligned with the European Agenda on Security, namely Serious and Organised Crime, Cybercrime and Counter-Terrorism.

In order to achieve maximum impact and operational results, Europol will dynamically adjust its operational delivery models and use of human resources. Existing and new operational capabilities and expertise will be employed as required to tackle the challenges in each of the key crime areas. Europol's Analysis Projects will support MS investigations in the area of Serious and Organised Crime within the priorities set in the EU Policy Cycle (2018-2021), while special focus will be placed in the area of facilitated irregular migration. The European Cybercrime centre will continue to drive and support intelligence-led actions and provide specialised forensic and technical support. In the area of counter-terrorism, Europol will focus on promoting and facilitating cooperation and information sharing with a view to improving the intelligence picture and increasing operational support to MS. In all priority

areas Europol will provide an effective platform for the coordination of operations carried out by MS.

A number of cross-cutting operational capabilities will also be used to support the MS. Europol will further develop and adjust Europol's analytical products to match the needs of the MS. Europol will further support the EU Policy Cycle and aim to increase its impact on the set priorities. The embedment of FIU.net at Europol and the work on asset recovery will aim to increase the use of Financial Intelligence in all crime areas while access to PNR data will allow for identifying further criminal links. Europol will also continue sharing its expertise and building capacity at Member States through its training and special tactics capabilities.

Europol will continue delivering in selected areas and as required by the Member States, central capabilities and expertise that are not available widely at national level, to provide cost-effective and enhanced support where a common European response to threats is required.

Europol will be prepared to swiftly adjust its response as required by MS and work more closely with front-line investigators, providing on-the-spot, real-time information exchange and expertise. Europol will aim to support MS by using the most suitable, tailor-made operational delivery models. Based on the assessment of MS needs, Europol's response could include short and longer-term deployments of Europol experts (e.g. through EU mobile investigation support teams or through deployment of Europol experts to CSDP missions or operations e.g. SOPHIA), forming situation centres to coordinate a response to major security events and crises, creating task forces or supporting the formation of multi-national teams to intensify efforts and achieve immediate operational results in areas demanding attention. Finally, Europol will establish the required connections and develop standard operating procedures or protocols, to be able to respond to emerging incidents.

2.1.   Support MS investigations in the area of Serious and Organised Crime

Europol has largely embedded the principles of intelligence led policing in its structure, processes and resources. The EU Policy Cycle priorities will be the main driver for operational support provided to MS in the area of Serious and Organised Crime. Additionally, Europol will support Member States' efforts in tackling hierarchically structured, poly-crime Organised Crime Groups ("Mafia-type" groups). The work on Intellectual Property Crime will also be enhanced through a cooperation agreement with EUIPO. Europol will continue its work of providing operational analysis, coordination and funding of operational meetings. Large-scale operations and joint action days will be coordinated from Europol HQ with the aim of achieving operational results. The clustering and reduction of the number of Analysis Projects and the exchange of best practices between them will serve to achieve consistent results and optimum allocation of human resources. From 2018 onwards, Europol will support Member States in tackling the priorities defined in the new EU Policy Cycle 2018-2021.

As part of the EU efforts to respond to the migration crisis the European Migrant Smuggling Centre (EMSC) established in early 2016 provides increased operational support to MS in their fight against organised people smuggling networks. The EMSC utilises a combination of operational capabilities to ensure the best operational support; the pre-existing Analysis Projects, JOT-Mare and regional task forces deployed at Migration hotspots were strengthened with EU mobile investigation and analysis support teams, providing on-the-spot operational and analytical support. The expertise of the EU Internet Referral Unit is also used to identify and refer online content relating to the provision of irregular migration services.

2.2.   Support MS investigations in the area of Cybercrime

In the area of cybercrime, one of the most dynamic and challenging threats faced by MS, Europol will deliver operational support to cybercrime investigations, in particular addressing those crimes i) committed by organised groups, especially those generating large criminal profits such as online fraud, ii) which cause serious harm to their victims, such as online

child sexual exploitation and iii) affecting critical infrastructure and information systems in the European Union.

The European Cybercrime Centre (EC3) will continue pioneering operational capabilities such as advanced digital forensic, technology tools and platforms supporting the MS in protecting society by providing a collective EU response to cybercrime. EC3 will also enhance its Victim Identification capabilities, in particular with regard to child sexual exploitation and continue its work in delivering prevention material.

EC3 will continue engaging with the law enforcement community, supporting the J-CAT and key partners, such as Interpol's ICGI, to identify, prioritise and coordinate operational action against cyber threats, becoming the EU reference for cybercrime investigators.

Increased cooperation with the private sector, academia and NGOs will be pivotal in acquiring multi-disciplinary expertise, promoting innovation and keeping up with the latest security and technological developments that act as facilitating factors for cybercrime.

EC3 will play an increasingly active role in the efforts of law enforcement against the use of encryption for criminal purposes.

2.3. Enhance cooperation in the area of Counter-Terrorism

In the area of Counter-Terrorism, more work is required to achieve better cooperation and sharing of information. Europol will work towards an intelligence-led, user-driven and sustainable approach to collaboration amongst EU MS, partners and Europol on counter-terrorism issues.

The European Counter-Terrorism Centre (ECTC), operational from 2016 at Europol, brings together Europol's existing capabilities to promote and build the necessary infrastructure to enhance information exchange and the ability to provide analytical and operational support in major investigations. A key role for the centre is to support major CT investigations of Member States.

The EU IRU will be used to tackle online radicalisation, while the increased capabilities afforded by the TFTP and the FIU.net will be used to enhance the intelligence picture on terrorism financing. Trafficking in firearms continues to be an enabler of various forms of serious and organised crime and has also emerged as a key concern in the wake of recent terrorist attacks. Europol will increase its support to Member States in the fight against trafficking in firearms. Similarly, it will continue in its efforts to help MS to combat violent extremism, including in relation to the protection of vulnerable communities.

Europol will continue the effort to apply secure, tailored solutions within its EIS and SIENA systems to promote and enhance information exchange in the area of counter-terrorism. From 2017, a 24/7 CT service is available within the Front Office of Europol.

Additionally, in case of a major terrorist incident, Europol will be able to provide a First Response Network to best support Member States' investigations.

2.4. Develop and manage high quality analytical support and an evolving portfolio of cross-cutting operational capabilities

Operational and strategic analysis will remain the basis of Europol's operational support. Analysis products will evolve in order to remain relevant with the aim to make best use of the information available to Europol to provide unique and valuable intelligence to Member States. This will include identifying the needs of Member States in terms of the type of analysis needed (e.g. tactical, strategic or operational), investing in the training of Europol analysts, further developing and maintaining quality standards for analytical support and exploring new methods such as big data analysis. Focus will also be placed on identifying and assessing future developments of crime. The new opportunities afforded by the integrated data management will ensure the provision of high quality value-adding analytical products.

Europol will step up its contribution in all stages of the EU Policy Cycle on organised and serious international crime. Europol will support the Policy Cycle priorities with the aim to improve the operational focus of operational actions and in addition, will provide Grants for the implementation of the actions. Finally, the coordination of cross-border investigations within the Policy Cycle priorities, including highly complex operations involving numerous operational actions, will be refined in order to identify the best ways to achieve operational impact.

The successful completion of the integration of FIU.net into Europol will present significant opportunities to increase the engagement of national FIUs in Europol's activities and to make better use of financial intelligence in national and international investigations in all priority areas.

Additionally, the use of financial intelligence in combination with other information such as PNR records can enhance the intelligence picture and provide the missing links to Member States in all priority areas; in this respect, Europol will assume an active role in PNR information exchange and gradually develop a travel intelligence capability.

Goal 3: Europol will be an efficient organisation with effective governance arrangements and a positive reputation

As of 1 May 2017, a new Europol Regulation is applicable.

As any organisation, in particular in the continuing climate of economic austerity in the EU, Europol aims at achieving the most efficient and effective use of all its resources (human, financial, facilities, ICT infrastructure and services). As a public organisation, Europol will continue adhering to the highest accountability and governance standards and will strive to introduce further efficiency gains in its processes.

Europol will continue to build its profile as a trusted partner in EU policing and promote the results of cross-border law enforcement cooperation in the EU. Finally, Europol will continue advocating for the needs of the European law enforcement community.

3.1. Ensure effective, efficient and accountable management of Europol's resources

Europol will remain vigilant in managing its human and budgetary resources in the most efficient way with a view to providing maximum operational support to Member States.

Further efficiency gains will be introduced through streamlining of reporting, processes and monitoring of resource allocation (human resources and budget).

ICT and building requirements will be significantly adjusted to support the vision and strategy while, at the same time, adhering to the strict security and data protection standards of Europol. A new ICT delivery strategy will ensure the optimisation of the delivery of ICT systems in line with business needs.

Europol will maintain its high accountability standards by addressing audit and evaluation recommendations and by adhering to its internal control standards. As a consequence of the Europol Regulation, Europol will be subject to new supervision and oversight from the European Data Protection Supervisor (EDPS) and the Joint Parliamentary Scrutiny Group (JPSG). In line with the European Union's policy, Europol will continue enhancing the transparency of its activities by facilitating access to documents through a public access register.

In order to best support Member States, Europol will continue to identify and develop the right staff competencies and skills and strive to obtain the best resources.

3.2. Promote the added value and achievements of EU law enforcement cooperation to stakeholders and EU citizens

Europol will continue to build its profile as a trusted partner in EU policing and promote the benefits and the value added from cross-border law enforcement cooperation to relevant stakeholders.

Based on on-going efforts Europol will take further actions to raise awareness about its services and the advantages of cooperation to law enforcement actors, decision-makers in the area of police matters and partners from other sectors.

As an EU Agency fostering European cooperation and integration, Europol carries also the responsibility to communicate the added value of its activities to the wider European public.

The joint work of the law enforcement authorities in the EU delivers results which are hard evidence of the added value and benefits that EU cooperation offers to citizens. Success stories of EU police cooperation become indispensable contributions to the positive shaping of citizens' perceptions towards law enforcement, the European Union and its activities.

Europol External Strategy 2017-2020

In order to strengthen Europol's contribution to consolidating the Security Union, in particular the fight against serious and organised crime and terrorism, Europol's activities in the external domain will focus on the following objectives:

- Optimising Europol's **partnerships**, operational and strategic;
- Strengthening Europol's role as the **preferred platform** for international law-enforcement cooperation against threats related to EU security;
- Reinforcing Europol's position within the **EU security architecture**;
- Promoting Europol's **successful cooperation model**.

1. Rationale

Article 12 of the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol Regulation) explicitly stipulates the establishment of a strategy for relations with **third countries** and **international organisations,** which is also an element of the multiannual overall strategic programming.

Europol's External Strategy, reflecting the Europol Regulation, does not cover cooperation with EU agencies and other partners, such as the private sector.

The Global Strategy for the European Union's Foreign and Security Policy (EU Global Strategy), the European Agenda on Security, followed by the Communication from the Commission delivering on the European Agenda on Security to fight against terrorism and paving the way towards an effective and genuine Security Union and the European Agenda on Migration, represent the basis of Europol's External Strategy for the years 2017 to 2020.

2. Goals

The goal of the External Strategy is to guide Europol's cooperation with third countries and thereby fulfilling the agency's objectives set by the Europol Regulation, which is to support the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

2.1. Contributing to the implementation of the EU strategic framework

As stated in the EU Global Strategy, the internal and external security is ever more interlinked. The European Union is expected to play a major role in providing a global security. Europol is firmly embedded in this framework.

Europol's external cooperation with core partners from the third countries, like-minded countries and regional groups will be based on operational requirements and the recognised need for effective law enforcement cooperation based on the above mentioned strategic EU documents.

In accordance with the priorities set by the EU's strategic documents in the area of internal security, such as terrorism, hybrid threats, cyber and energy security, organised crime and external border management, **Europol's recognised operational priorities in the context of this strategy will be mainly in the area of serious organised crime, cybercrime and terrorism.** Hybrid threats are a new phenomenon which has to be further analysed in order to define Europol's role and the possible support it could provide in response to this global threat.

2.2. Implementation of the Europol External Strategy

Europol's external relations should primarily focus on **strengthening Europol's contribution** to the fight against the three areas of crime identified in the European Agenda on Security: **Serious and Organised Crime, Cybercrime and Terrorism.** Among serious and organised crime challenges, **migrant smuggling** is of particular importance.

Europol's external activities are and will continue to be driven by **operational needs**. They should in particular serve the proper implementation of actions planned under the **Policy Cycle** and foster involvement and active participation of partners – third countries and organisations - in **EMPACT** activities.

Member States remain the leading participants of EMPACT and the mechanism itself primarily serves the internal security of the EU. However, its full and successful implementation, in particular at the operational level, is not possible without close partnership with third states and organisations. Europol will prioritise cooperation with partners that contribute to the implementation of the Policy Cycle.

At the same time, Europol will react flexibly to new or emerging security threats.

3. Objectives

Europol's objectives in the external relations domain are as follows:

3.1. Optimising the **network of partnerships**, operational and strategic

Europol's primary objective is to ensure proper exchange of information and strengthening its role as the **EU criminal information hub**. This can be achieved through strategic and operational partnerships with external partners in accordance with the Art 23 and Art 25 of the Europol Regulation.

3.2. Strengthening Europol's role as the **preferred platform** for international law-enforcement cooperation against threats related to EU security

Europol should continue to offer its partners an **attractive environment for cooperation**, both bilateral and multilateral**.**

The community of **liaison officers** attached to Europol plays a crucial role in facilitating proactive and coordinated activities against the serious crime. It will remain **one of Europol's unique features**. Europol's partners that contribute to its activities, in particular to its operational tasks, should have the opportunity to benefit from this unique feature and second their officers to Europol. Partners already having their officers seconded should be encouraged to develop their liaison bureaus further, involving various services that might benefit from and contribute to Europol's work. Secondment of counter-terrorism and cybercrime liaison officers should be particularly encouraged.

The development of the liaison officers' network should lead to better and more coordinated international police cooperation, bringing various states and regions closer together; the role of Europol in facilitating trans-Atlantic cooperation should be seen as an example in this regard.

Promoting **SIENA** and the **universal message format** will further contribute to secure and swift information exchange which, if necessary, might be combined with Europol's analytical capabilities.

Europol's Platform for Experts (EPE) should be promoted further in this context, as it offers a secure cooperation environment bringing together security experts. EPE should remain open to those partners with which Europol does not cooperate otherwise.

3.3. **Reinforcing Europol's position within the EU security architecture** , in order to address external threats to the security of the EU

Europol is one of the key actors of the EU internal security architecture and an important part of a coherent European response to external security challenges like terrorism or migrant smuggling. Europol will strive to further develop its contribution to EU security, especially in the field of external relations.

Europol will further **strengthen cooperation with the European Commission and the European External Action Service** in order to ensure the proper exchange of strategic information, to provide joint analysis of threats that have both an internal and external dimension and to facilitate contacts with third countries with which Europol doesn't cooperate yet.

Europol will further develop its cooperation with **EU operations and missions**, in particular those having executive functions and those operating in areas relevant for the internal security of the EU.

Europol will assess the potential of temporarily **deploying its staff outside of the EU, including to EU delegations, missions and operations**, which could contribute to gathering intelligence related to serious threats, such as migrant smuggling or terrorism.

Europol's role in **capacity building** in third countries will remain limited, focused on areas in which Europol has specific expertise and which are relevant for Europol's core business. Any capacity building activities should be carefully assessed and planned, with due consideration to available resources.

3.4. Promoting Europol's **successful cooperation model**

Regional entities that facilitate international police cooperation might benefit from Europol's successful cooperation model. Subject to available resources, Europol will promote and explain its functioning, its successful cooperation mechanisms and the lessons learned. The objective is to facilitate future cooperation between those regional entities and Europol.

4. Partners

The Europol Regulation gives Europol possibilities for effective and mutually beneficial cooperation with third countries and organisations. It gives Europol a global reach to serve the European law enforcement community.

When choosing cooperation partners, geographical criteria need to be combined with others, as for certain types of crime the geographical proximity of a cooperation partner is not the only criterion.

4.1. Third countries

As foreseen in the Regulation, agreements concluded before 1 May 2017 will remain the basis for future cooperation. Europol will strive to maintain and further develop the **already existing relationships** with all partners that are parties to agreements already are in force.

The Europol Strategy states that Europol will aim to further strengthen its partnership with third states. The United States, Mediterranean countries and the Western Balkans are explicitly mentioned.

The United States of America will remain Europol's key partner. Mutual support and operational cooperation should be further reinforced, in particular through the increased exchange of information and active involvement in operational activities. Terrorism and cybercrime will remain main areas of common interest, notwithstanding continued cooperation in other fields, such as organised crime and migrant smuggling.

The migratory crisis and present terrorist threat call for closer cooperation between Europol and **Middle East and North African** countries. Each country of the region has its own specificities and a unique position in the security environment. In developing Europol's cooperation in this region, close cooperation with the European Union External Action Service is of particular importance.

The **Western Balkans** will remain a region of particular relevance for Europol. Europol has been prioritising cooperation with the region for many years, which led to the conclusion of numerous operational agreements and successful strategic and operational cooperation. Further implementation of the agreements and full use of the already available mechanisms remain crucial. Migrant smuggling, organised crime and terrorism will remain key areas of common interest.

Europol will continue supporting **regional initiatives in the Western Balkans**, as long as their activities supplement and enhance Europol's operational cooperation with the region.

The above mentioned areas will also require close cooperation with **Turkey,** the development of which depends on the general relations between the EU and Turkey.

Europol recognises the importance of cooperating with **Asian countries**, such as **India** and **Pakistan**, and will strive to strengthen cooperation with them.

Given the impact of Chinese organised crime on the EU and the high international profile of Chinese criminal groups, building cooperative relations with **China** will be of particular importance.

South- and Central American states will be important partners, in particular as regards drug-related crime. Furthermore, options available for cooperation under the Europol Regulation will be explored for the bilateral relations with **Israel** and **the Russian Federation**.

4.2. International organisations

Interpol will remain Europol's key partner. Respective capabilities and tools are complimentary and Europol remains **focused on supporting EU Members States** and ensuring **EU-wide** law enforcement cooperation. In view of the global challenges the EU is facing, cooperation with Interpol will remain particularly relevant and will be enhanced through closer alignment, increasing joint participation in operational activities and setting of common strategic activities.

Europol will make efforts to enhance its cooperation with **other international organisations** that play a role in the field of security, such as United Nations/ United Nations Office on Drugs and Crime (UN/UNODC), Organisation for Security and Co-operation in Europe (OSCE), World Customs Organisation (WCO) or North Atlantic Treaty Organization (NATO). Europol will strive to strengthen its cooperation in particular with the latter; counterterrorism and tackling migrant smuggling are detected to be the fields of common interest.

Europol is open for cooperation with **regional police cooperation organisations** such as Ameripol, Aseanapol and Afripol. Cooperation mechanisms should reflect operational needs as well as geographical and thematic priorities of Europol. Europol will strive to promote its successful cooperation model to foster regional cooperation.

5. Oversight mechanism – the role of the Management Board

The Management Board adopted guidelines on the implementation of the External Strategy in its meeting of 1 May 2017.

Information on the implementation of the External Strategy will be presented to the Management Board every six months. Moreover, Strategic Reviews concerning particular partners or regions will be submitted to the Management Board on a regular basis in order to present the on-going cooperation and seek guidance on further actions.

3.   Human and financial resource outlook for the years 2019-2021

The Multi-annual Financial Framework (MFF) 2014-2020 of the EU had prescribed in 2013 a net reduction of Europol's resources for the years 2014-2020. In 2016, however, the political priorities of the EU made a necessary shift towards the establishment of a Security Union in order to address a number of pressing issues, particularly the increased migratory flows, the elevated terrorist threat, cybercrime or internet-facilitated crime and the fragmented EU information landscape.

In the context of the Security Union, Europol's role in the security landscape of the EU was discussed with increasing intensity and as a result, Europol was entrusted with a number of entirely new functions such as the European Cybercrime Centre, the European Migrant Smuggling Centre, the European Internet Referral Unit, the European Counter-Terrorism Centre and the FIU.net. Though some resources were provided to Europol to perform these new tasks, Europol has depended heavily on internal re-allocation of operational staff and on the shifting of posts from support functions to the Operations Department.

The discussion of Europol's role in the Security Union including on the latest topics such as innovation, interoperability[7] and decryption, calls for a continuous and comprehensive review of the agency's overall needs for human resources. In order to be able to perform the tasks assigned to it, Europol has to be reinforced with an appropriate level of human and financial resources.

Europol is an operational law enforcement agency, supporting the Member States by participating in their operations be it with expertise, analysis, on-the-spot deployments, cross-checking of data and operational meetings among other activities. Therefore, as criminal and terrorism threats are rising and EU cooperation becomes increasingly a vital success factor, the demand for Europol's services continues to grow and requires a corresponding increase in the agency's handling capacity.

Europol sees the necessity for further growth and development over the coming years (2019 – 2021). A small sample of the developments that most affect the security of EU citizens and for which Europol would require further development and resources are:

- Prevent or respond to terrorist attacks
- Take more terrorism propaganda offline
- Increase pressure on smuggling and trafficking networks, including via being present at migration hotspots in affected MS with Guest Officers
- Pioneer law enforcement information processing solutions of the next generation
- Increase capacity of centralised support for cyber forensics and decryption
- Increase the use of financial intelligence in investigations
- Develop a strong victim identification capability particularly to protect children from sexual abuse and exploitation

In its previous Programming Document Europol clearly defined its ambitions in a comprehensive plan for the years 2018-2020 in which an annual staff increase of approximately 70 Temporary Agent posts was foreseen. Eventually a more modest staff increase for 2018 was decided upon by the budgetary authority which amounted in a net staff increase of 26 Temporary Agent posts.

In the current Programming Document 2019-2021 Europol has based its planning on the modest approach taken by the budgetary authority for 2018 assuming that a bigger resource demand would not be met, and as approved by the Management Board it requested 43 new posts. The new posts are needed, among others, in order to enable continuation of operational support to Member States at an acceptable level, to boost to a certain extent the area of innovation and operational ICT and also to allow the agency to keep up with increasing operational demand from Member States, for example to take into account a

---

[7] COM(2017) 794 final

constant growth of support requests in the area of strategic and operational meetings that are organised for Member States.

It is important to stress the focus placed on augmentation of ICT resources. Information management capabilities are at the core of Europol's mandate and mission. In the last five years alone, Europol has been accepting at least 15% more contributions of operational data by MS each year, going from around 26,000 contributions in 2012 to more than 70,000 in 2017. During the same period the number of objects in the Europol Information System (EIS) has increased <u>fivefold</u> to containing more than 1 million objects in 2017. Member States have also intensified their usage of EIS – querying the system more than 2 million times in 2017- while more than 1,000 competent authorities are communicating through Europol's SIENA. Beyond the increased information exchange and number of users, technological solutions are continuously being developed and their services used to support the Member States, such as face recognition and victim identification solutions. Finally, Europol is committed to upgrading its information management and systems architecture and to introducing up-to-date, innovative capabilities to ensure that the information shared by Member States results in analysis products that provide the most accurate and comprehensive intelligence picture. This requires transformational as well as incremental change, and commensurate investments.

In past years, the budgetary process has resulted in Europol receiving additional resources specifically for its Operations Directorate, i.e. mainly analysts and specialists with crime analysis and investigation expertise. However, during the same period Europol's ICT capabilities did not see the investment that would be expected to keep up with the growth of demand for the organisation's products and technological developments in the field of information management. It is therefore imperative and long overdue to make a structural correction to the distribution of additional resources to the agency.

These staff increases, together with the necessary investments in the building and for operational and ICT initiatives, and the inclusion of funds to continue the secondary security checks at the hotspots via Europol's budget instead of via grants, lead to a necessary budget growth of € 8.1M in 2019 (total € 138.3M) compared to 2018. For future years there are increases foreseen as in particular building related investments will be a lot less in 2020 (total € 146.1M) and 2021 (total €152.0M).

HUMAN RESOURCES

From a high level perspective, for the next three years, Europol foresees the following Temporary Agent staff increases:

Area of the business	2019 requested	2019 provided*	2020	2021
Operations Directorate	+19	+4	+19	+16
ICT Department	+20	+9	+14	+12
Governance and Administration	+4	+2	+4	+3
Total	**43**	**15**	**37**	**31**

*The allocation of the posts in 2019 is preliminary at this stage. Final allocation of the posts in 2019 is pending on the outcome of the reorganization proposal to be presented to the Management Board in February 2019.

From the requested 43 posts for 2019 the final Europol Budget 2019 granted the agency with 15 new posts only. This implies that some of the planned actions for 2019 (those marked with asterisk indicating a dependency on additional resources) in Section III will be implemented to a limited extent or might need to be deprioritised.

Temporary agents
Starting from the 2017 establishment plan of 550 posts the net number of posts increased by 26 and comes to 576 for 2018 (+ 4.7%). For 2019 an increase of 15 posts is provided.

Contract Agents
In response to business needs, the number of contract agents increased in 2017 to 165 full time equivalent (FTE) posts (153 heads at the end of 2017) which was possible as a consequence of budget availability. For 2018 the FTEs are envisaged to further increase to 212 also taking into consideration a switch from contractors (budgeted under Title 3) to Contract Agents (budgeted under Title 1) for certain ICT tasks (increase of 16 CA posts). From 2019 the number of contract agents is increased to 232 taking into consideration the impact of the move of part of the organisation to a satellite building to overcome the office space constrains.

Seconded National Experts
The number of Seconded National Experts (SNEs) is foreseen to remain stable at 71. Considering the challenges that Member States have to make SNEs available and also taking into account the strong support by Member States for Guest Officer SNEs for deployments at hotspots, it is considered that going beyond the current levels is not feasible.

A breakdown of the areas of the business and what new posts are needed for and will be specifically used for (to the extent to which they are provided) is described in this section. For detailed data and numbers per staff category, see Annex III.

In Operations Directorate:

Horizontal Operational Services (incl. the 24/7 Operational Centre)
The reinforcements for Horizontal Operational Services are foreseen for the 24/7 support, for the Financial Intelligence Group, for EMPACT and cross-cutting support, for analysis and training coordination and for additional analysis capacity. 2019 will be also a crucial year for the establishment of Europol's capabilities in the area of travel intelligence and the setting-up of the Europol Travel Intelligence Centre (ETIC).

European Serious Organised Crime Centre (incl. EMSC)
The posts for ESOCC are meant to reinforce the Weapons and Explosives clusters and the Drugs cluster in line with the ambition of the new Europol Drug Strategy. Specifically for the EMSC new posts will contribute to the delivery of the objectives of the Malta Implementation Plan and in particular to the strengthening of cooperation with the MENA countries, including the setting-up of a Clearing House and Regional Cooperation and Implementation Platforms. The provision of adequate support to MS in the framework of the EU Policy Cycle priorities and especially the new priorities will be also reinforced with additional resources.

European Cyber Crime Centre (EC3)
The posts for EC3 are focussing on digital forensics, big data analytics, black market sites (Dark Web and Open Web), cross-departmental encryption support, victim identification, child sexual exploitation, public-private cooperation, cyber bridge function towards global taskforces and further support towards the Joint Cybercrime Action Taskforce. In particular, Europol will aim at further developing and utilising its potential to perform as a European centre of expertise on decryption.

European Counter Terrorism Centre (incl. EU IRU)
The posts for the ECTC will deal with Genocide, Crimes against Humanity and War Crimes, PNR, OSINT monitoring, IRU referrals and check the web, translations, analysis and R&D coordination. Specifically, the tasks arising for Europol from the EU Internet Forum Action Plan to Combat Terrorist Online Content will require the utilisation of additional resources.

In ICT Department:
The posts are primarily envisaged for innovation profiles ranging from data-lake and cognitive computing operators, technical product managers, solution developers, smart

capability testers to data enrichment scientists. In addition, software factory engagement managers and capacity for the implementation of IDMC and Business Product Management for the other operational systems are planned. New ICT posts remain crucial for delivering on the mid-term ICT programmes (NEO for operational projects and nGage for optimisation and efficiency of corporate administration and support processes) established in 2017, which have been hit by a lack of new resources in both 2017 but particularly in 2018. As mentioned above, in addition to the requested posts, the posts envisioned in the Commission's proposal on interoperability, will be used to increase the performance of Europol's systems as to make them part of the interoperability landscape.

In Governance and Administration:
The posts will be used to ensure that the governance and administration capacity stays up to speed with the operations. Staff cuts from last years were for a large part taken by this area while at the same time the previous enlargements for EC3, the ECTC and the EMSC resulted in additional workload. Conversion of local staff into TAs and CAs is foreseen as well as the setting up of a new medical service.

Rate of absorption of additional resources 2019-2021
The sooner Europol is reinforced with the resources it needs to develop its current and future tasks, the bigger impact it can have by providing operational support to the MS. At the same time, Europol recognises that the resources required would be difficult to absorb in just one year and in all areas. The reinforcement of Europol should be done in a way in which there is flexibility to assign the posts within the organisation to best tackle the highest and most urgent priorities, while taking into account recruitment needs to replace existing posts (the turnover rate of Europol can be significant, given the policy of the Agency regarding restricted posts and the rotation principle).

As per best practice, the following principles on priority would continue to apply:

- Posts related to preparing the infrastructure of the organisation to handle the operational growth will be filled in first. These can include supporting posts needed for immediate handling of staff growth (e.g. recruitment, facilities) and ICT posts (e.g. implementing IDMC and interoperability changes, developing tools for operational support, responding to growing demand for support to operations i.e. more systems and more users).

- Operational posts:
  - Posts for vacancies (resignations, end of contract) where there is disruption of service;
  - Posts for new tasks at a rate that allows for swift absorption of staff;
  - Posts for growing tasks to allow for a balanced response to Member States demands.

- Other governance and administrative support posts will be filled at the rate dictated by the growth of the organisation.

Staff cuts / redeployments
The staff cuts for both the initial 5% and for the additional 5% for the re-deployment pool are implemented as planned. Out of a total of 45 posts to be reduced there were 36 posts cut at the end of 2017.

An important factor that was not taken into account in the requirement of staff cuts was that Europol, unlike other EU Institutions and Agencies, was already working on a 40hr week schedule, therefore not being able to recuperate some of the cuts by the increase in working time introduced in 2014 with the new Staff Regulation.

Efficiency gains
Europol continues to strive towards being a more operational agency. In 2017, the results of the job screening exercise show a small increase in the percentage of operational jobs and small decreases in the percentages for neutral and administrative/coordination jobs.

The job screening exercise was done for the fourth time in 2017, according to the guidelines defined by the EU Agencies Network and based on all people working at Europol's premises on 15 December 2017. This not only includes Temporary Agents, Contract Agents and SNEs

but also Europol Liaison Officers, trainees and external service providers based at Europol's premises.

Compared to 2016, the Operational Jobs have increased by 1.6 points to 76%. On the other hand, the jobs dealing with administrative support and coordination have decreased by 1.3 points, to 19.6%. Neutral jobs have decreased by 0.3 points to 4.4%.

Job Type category	2016 Jobs	2016 (%)	2017 Jobs	2017 (%)	Δ 2017
Administrative support and Coordination	**227**	**21%**	**230**	**20%**	**-1.3%**
Administrative support	164	15%	166	14%	-1.0%
Coordination	63	6%	64	5%	-0.3%
Operational	**808**	**74%**	**891**	**76%**	**1.6%**
General Operational	591	54%	668	57%	2.5%
Programme Management	193	18%	200	17%	-0.7%
Top level Operational Coordination	24	2%	23	2%	-0.2%
Neutral	**50**	**5%**	**51**	**4%**	**-0.3%**
Finance	50	5%	51	4%	-0.3%
	1,085		**1,172**		

Staff financed with ad hoc grants

For the years 2019 and 2020 Europol will also have a number of Contract Agents and SNEs which are directly funded via ad hoc grants.

Grant from EUIPO: 6 SNEs and 2 Contract Agents (current grant until 31/12/2019)
Grant from DG FPI: 7 Contract Agents
Grant from DG Near for deployment of Liaison Officers in the Western Balkans: 4 Contract Agents

FINANCIAL RESOURCES

Revenue:

The total revenue for 2019 comes to € 138.3M. This amount includes the subsidy for the European School in The Hague (ESH) of almost € 2.3M.

Item	Heading	Revenue 2017	Revenue 2018	Final Budget 2019
9000	Regular subsidy from the Community	113,009,613	120,448,520	136,032,458
9001	Subsidy from Community for Type II School	1,614,000	1,797,000	2,273,000
9010	Other subsidies and grants	-	P.M.	P.M.
9101	Denmark contribution[8]	-	P.M.	P.M.
9200	Other revenue	-	P.M.	P.M.
	TITLE 1 — TOTAL	**114,623,613**	**122,245,520**	**138,305,458**

Expenditure:

Item	Heading	Budget outturn 2017	Budget 2018	Final Budget 2019	% of the budget
1	Staff	71,864,946	81,002,493	84,205,258	61%
2	Other Administrative Expenditure	9,782,622	10,837,038	14,095,700	10%
3	Operational Activities	32,655,720	38,405,990	40,004,500	29%
	Total expenditure	**114,303,288**	**130,245,520**	**138,305,458**	**100%**

---

[8] It is envisaged that the budget will be amended later in the year with an additional contribution from Denmark via a separate procedure. Those funds will be handled as external assigned revenue (fund source R0).

The Final Budget 2019 increases by € 8.1M (or 6.2%) compared to the Budget 2018.

The provisional reflection of the breakdown per activity (Activity Based Budgeting) provides the following overview per goal which shows that 76% of the planned budget will be allocated for direct operational support (Goal 1+2):

Goal	Europol Work Programme	Final Budget 2019	%
1	To be the EU criminal information hub, providing information sharing capabilities to law enforcement authorities in the MS	48,690,189	35%
2	To provide the most effective operational support and expertise to MS investigations by developing and employing a comprehensive portfolio of services	57,019,593	41%
3	Europol will be an efficient organisation with effective governance arrangements and a positive reputation	32,595,676	24%
	Total expenditure	**138,305,458**	**100%**

Title 1 – Staff expenditure:

The estimated staff expenditure amounts to € 84.2M and represents 61% of the total budget. It reflects a 4% growth compared to 2018 which will be used for the additional staff and the salary and weighting increase (effective 1 July 2018).

The number of Contract Agents increased in 2018 and is expected to further grow in 2019 as their employment is a valuable and efficient option to support activities in an environment with ever increasing demand. In 2019, these services will be employed in particular for the temporary satellite building.

The staff and salary budget foresees the expenditure for overall numbers of 591 TAs and 232 CAs. The direct salary and allowances related budget (including recruitment expenditure and relocation allowances) for TAs and CAs (Chapter 11 – Staff in active employment) comes to € 77.8M, an increase of € 2.6M compared to the year 2018.

An increase of the budget (€ 616K compared to 2018) is also estimated for other staff related expenditure such as medical and PMO services, other external services (outsourced activities for removal and hospitality services, additional security officers and AV support) and the costs for the European school.

Title 2 – Other Administrative Expenditure:

The final budget for administrative activities comes to € 14.1M and represents 10% of the total Europol budget.

A significant increase of € 3.3M or 30% compared to the Budget 2018 is due to the ongoing activities for the SHR (overall € 4.3M is planned for 2019 for the SHR of which € 3.8M under Title 2). The SHR is planned via three different initiatives:

- Increase the workplace and meeting capacity in the headquarters (mid-term housing solution);
- Temporary satellite building for approximately 190 staff members; and
- Permanent expansion of the headquarters (long-term housing measures).

Another element concerns building-related running costs, other facilities expenditure and investments regarding user elements of the building amounting to € 5.8M. This encompasses € 4.1M for facilities expenditure and investments concerning user elements of the building for ongoing running facilities expenditure, including the implementation of the service level agreement with the Host State (contractual maintenance to retain the current service environment and business continuity of the headquarters and involved infrastructure). In addition, € 1.7M are for other running costs (rent of the data recovery site, energy, cleaning, insurance, security equipment and services, etc.).

The budget for administrative ICT amounts to € 1.8M for ngAGE (next generation Administrative and Governance Environments), which includes continuation of support tools and systems, such as IRIS (Intranet), FMIS (Facilities Management System), ABAC (the Commission's financial system), e-Procurement and for the roll-out of Sysper II, the Commission's HR System.

An amount of € 2.1M is foreseen for the continuation of other governance and administrative expenditure such as open source and database subscriptions, legal expenses, administrative expertise, uniforms, furniture, car fleet, office supplies, postal and courier services, telecommunications, etc.

The budget for activities of the Management Board and its Working Groups have been kept at a similar level as in 2018 and amounts to € 600K.

Title 3 – Operational activities:

The estimated operational expenditure adds up to € 40M and represents 29% of the total budget. When excluding the Decryption Platform initiated via an amending budget in 2018, and which will continue together with DG JRC in 2019, the increase for operational activities compared to 2018 amounts to € 6.6M or 19.7%.

A budget of € 14.9M for Chapter 30 – Operations, emphasises Europol's continued focus on operational results and increasing support to Member States. The budget is foreseen to further continue supporting Member States' activities under the EU Policy Cycle by awarding grants (€ 4M); in addition, it will allow for the continuation of security checks at hotspots (€ 3M), while also a significant part will still be used to support Member States in organising operational and strategic meetings.

The budget for operational ICT services and programmes under Title 3 (Chapters 31 and 32 together) comes to € 20.7M, which is an increase of € 4.6M compared to 2018. This budget prominently includes the New Environment for Operations programme, which drives Europol's evolvement from collecting to connecting operational information, integrating innovative technologies like machine learning and artificial intelligence, and for advancing Europol's information management architecture in line with the integrated data management concept (IDMC).

Part of the operational expenditure is intended to cover the allowances for the Seconded National Experts, amounting to € 4M for 71 SNEs.

The budget for high level external stakeholder meetings (HENU and Europol Police Chiefs Convention) amounts to € 390K.

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.

- 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
Goal 1: Europol will be the EU criminal information hub, providing information sharing capabilities to law enforcement authorities in the MS		
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.

Strategic Objective 2016-2020	Europol WP Activity	Objective 2019
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.
Goal 2: Europol will provide the most effective operational support and expertise to MS investigations by developing and employing a comprehensive portfolio of services		
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.

Strategic Objective 2016-2020	Europol WP Activity	Objective 2019
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.
Goal 3: Europol will be an efficient organisation with effective governance arrangements and a positive reputation		
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[9].

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

---

[9] COM(2017) 794 final

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

Core operational ICT capabilities, specialised systems and tools and key IM initiatives
Development, implementation and/or maintenance of capabilities[10]:   o Messaging Capability incl. Secure Information Exchange Network Application (SIENA); Universal Message Format (UMF);   o 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);   o Data Acquisition Capability incl. Large File Exchange (LFE); Decryption Platform;   o Data Management Capability incl. Unified Search Engine (USE); Unified Audit System (UAS) for data protection;   o Analysis Capability incl. Europol Analysis System (EAS);   o SMART Capability incl. Automated Biometrics Identification System (ABIS); Face Recognition system (FACE); Enhanced Risk Entities Solution (ERES) and machine learning;   o Knowledge Sharing Capability incl. Europol Platform for Experts (EPE);   o 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);   o Technical Infrastructure Capability incl. Identity and Access Management (IAM);   o Operations Support Capability incl. European Tracking Solution (ETS); Mobile Office.   Connectivity and support to: o Schengen Information System (SIS II)   o Visa Information System (VIS)   o Eurodac   o Passenger Name Records (PNR) network   o Prüm framework

Main tasks
Business product management of Information Management systems   o Represent and advocate for end users' interests;   o Manage the product lifecycle from concept to phasing out;   o Perform business analysis;   o Identify new opportunities, product enhancements and extensions;   o Identify, specify and prioritise features, functionality and capabilities;   o Act as a Senior User in ICT projects;   o Facilitate the design, development and launch of new versions of the product;   o Promote product awareness and deliver training;   o Support end users, including the facilitation of issue resolution;   o Carry out standard configuration changes;   o Report on product usage;   o Develop, maintain and execute product roadmap;   o Develop expertise and keep up to date with technological advances;

---

[10] The list represents an initial mapping of operational ICT capabilities and the corresponding solutions.

o Facilitate the development and implementation of high impact and differentiated product positioning;
o Manage business cases for establishing access to relevant EU information systems;
o Contribute to the work on interoperability and connectivity of IM systems at EU level;
o Represent Europol in relevant committees and boards, e.g. SIS II, VIS, EURODAC, EES, UMF, DAPIX and ADEP.

Embedded ICT Security

o Define and monitor security standards;
o Check ICT infrastructure for weaknesses;
o Design and build ICT security improvements;
o Handle security-related calls;
o Enable and enforce secure software coding best practices in software development;
o Review solutions, spot security issues and propose improvements;
o Define and implement security processes and procedures, including staff training;
o Perform audits on implementation of the security processes and procedures;
o Define roadmap and necessary steps to ensure ICT continuity.

Solutions Operations

o Daily / periodic maintenance of the solutions and infrastructure;
o Own and evolve monitoring & response operations practices;
o Create and periodically test backups;
o Maintain the Configuration Management Database for all non-work place services related systems and components;
o Patch periodically all network, server, storage, middleware and application components;
o Implement technical product manager roles for all commercial off-the-shelf solutions.

Solutions Deployment

o Define and manage the Change and Release management processes;
o Implement all changes into all environments of the Europol ICT landscape;
o Develop and maintain processes and tooling for automated deployments;
o Provide tools to be used during the software development cycle;
o Own the Team Foundation Server system (or equivalent) for deployment in Production, Staging and Test.

Law Enforcement Accelerated Provisioning

o Coordinate the provisioning of ad-hoc capabilities to support LE operational needs;
o Engineer and deploy ad-hoc processing environments;
o Engineer and implement data pre-processing tools;
o Identify opportunities for reuse, and define new services when appropriate;
o Guarantee security and data protection considerations.

Application Delivery Services

o Provide application development services across multiple delivery models (e.g. external software factory);
o Ensure consistent software engineering practice (including secure coding);
o Define delivery methods, tools and standards.

Test & Quality Assurance

o Own the quality assurance processes and standards;
o Perform functionality, continuity and security testing related to software solutions and infrastructure changes;
o Continuously develop an automated testing approach.

ICT Solution Architecture & Engineering Coordination

o Own the overall Solution Portfolio;
o Ensure that ICT solutions are aligned with the intended capability portfolio;
o Own the end-to-end design of individual solutions;

---

o   Provide services to implementation projects;
o   Create enabling technology roadmaps, including replacement of obsolete solutions;
o   Proactively identify and propose technology-driven innovation opportunities.

Portfolio and Project management

o   Create ICT Workplan and monitor its execution;
o   Ensure that the projects and work packages deliver according to agreed schedule, scope and cost;
o   Proactively identify and manage risks, perform stakeholder management and relevant communication to involved parties;
o   Support key projects with technical expertise;
o   Coordinate ICT work planning capacity; validate estimations and assumptions.

ICT Capabilities Innovation

o   Maintain the portfolio of ICT capabilities and business solutions, and their respective roadmaps, while ensuring evolution in alignment with business needs and strategy;
o   Analyse business capabilities and needs, propose opportunities for ICT innovation, and drive architectural decisions;
o   Establish requirements for ICT solutions aligned to business needs and the Business and Information Architecture;
o   Analyse processes and user interaction to support development and procurement initiatives with the appropriate set of solution requirements;
o   Propose functional design to reach the optimal implementation considering business needs and technical capabilities.

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

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.

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

---

[11] Indicators marked in italics are the Corporate Key Performance Indicators.

Indicators[11]	Latest result Q3 2018	Target 2019
Number of SIENA messages exchanged	813,306	1,190,000
Number of SIENA cases initiated	56,231	88,000
% of all SIENA messages received by Europol containing structured data	13%	15%
Number of objects in the EIS (MS+Europol)	1,217,667	1,500,000
Number of person objects in the EIS	196,576	240,000
Number of EIS searches	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
o Monitor operational data on 24/7 basis as the single point of entry for any incoming information from stakeholders; o Decide on the acceptance of information into Europol's databases; o Assign (distribute) operational messages within the Operations Directorate; o Process and handle non-priority cases and manage related information hits including evaluation and reporting (cross-matching); o Process and handle urgent messages in priority cases, in close cooperation with competent analysis projects; o Process biometric data;

o Provide permanent monitoring and reporting of Open Source information;
o Manage EIS operational data including the insertion of data on behalf of third parties and hit management;
o Manage operational information exchange with third parties.

Support of Operations

o 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;
o Maintain organisational overview of on-the-spot deployments;
o In close cooperation with the Special Tactics team and other departments, guarantee 24/7 access to expertise and specialised operational knowledge;
o Manage the overview of mobile offices and other operational equipment;
o Manage the operational rooms;
o Support the coordination of operations and large-scale joint actions; Organise and chair corresponding planning meetings;
o Provide remote support to on-going actions/operations/major international events/on-the-spot deployments.

Initiating immediate actions and crisis response mechanisms

o 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;
o Provide support to crisis management during serious incidents;
o Coordinate Europol's immediate response together with other relevant units and stakeholders;
o Initiate specialised assistance;
o Liaise with Europol's partners (MS and third parties) affected/involved.

Business Intelligence

o Prepare weekly intelligence briefing reports to inform internally about main operations, trends and patterns;
o Maintain dashboards for management to provide business information for decisions;
o Monitor on 24/7 basis information flow, requests for operational support and open sources to enable fast information to management when necessary;
o Further develop, maintain and deliver the 3-month induction training for newly recruited analysts; Contribute to the delivery of the EIS and SIENA trainings;
o Host visits to the Front Office operational rooms.

Strategic cooperation

Strategic cooperation with MS

o Manage strategic cooperation of Europol with MS;
o Coordinate Europol participation in the Management Board (MB);
o Coordinate and prepare meetings of the Heads of Europol National Units (HENUs);
o Organise study weeks for staff from Europol National Units;
o Support the liaison officers' community based at Europol, including by facilitating regular Heads of LB and Heads of Desk meetings;
o Support the Joint Investigation Teams (JIT) including the provision of funding in cooperation with Eurojust.

Strategic cooperation with third countries

o Manage strategic cooperation of Europol with third countries;
o 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;
o Support the implementation of the operational agreement with the USA and manage the Liaison Office in Washington;

o 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;
o Manage the deployments of Europol's Liaison officers to the Western Balkans;
o Monitor the implementation of agreements and the fulfilment of obligations and commitments.

Strategic cooperation with EU institutions, agencies or bodies

o Manage strategic cooperation of Europol with EU institutions, agencies or bodies; manage the Liaison Office in Brussels;
o Provide (technical) advice and contribute to the implementation of new EU political and legislative initiatives;
o Support the implementation of the operational agreements with Eurojust and Frontex;
o Support the implementation of the strategic agreements with CEPOL, ECB, ECDC, EEAS, EMCDDA, ENISA, EUIPO, EU-LISA, the European Commission and OLAF;
o Collaborate with other relevant EU agencies such as EASO, EMSA and FRA, and contribute to the work of the JHA Agencies Network.

Strategic cooperation with international and regional organisations

o Manage strategic cooperation of Europol with international organisations;
o Support the implementation of the operational agreement with Interpol and manage Europol's Liaison Offices in France and Singapore;
o Support the implementation of the strategic agreements with UNODC and WCO;
o 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.

Legal services - EU and International Law

o Provide legal advice on the implementation of Europol's legal framework and data protection rules;
o Advice on legality and compatibility of new Europol initiatives with EU law, as well as on new EU initiatives having an impact on Europol;
o Implement the external relations regime as per the Europol Regulation;
o Conclude Administrative and Working Arrangements;
o Upon request provide assistance to the Commission's negotiations of international agreements and / or input to the process of preparing adequacy decisions;
o Provide legal advice on new possibilities for case by case cooperation with any third country, in the absence of an agreement or adequacy decision;
o Conclude undertakings from third countries, international organisations and EU bodies exchanging personal data with Europol;
o Implement and guide on new possibilities for cooperation with private parties stemming from the new Europol Regulation.

2019 Objectives

A.2.1. Broaden the information processing capabilities of Europol's Front Office.

Actions	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.
	Maintain the Front Office capacity to respond to MS requests in an expeditious way.*
	Ensure the efficient management, including the application of clear prioritisation criteria, of an extensive fleet of Mobile

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.

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.

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

Accommodate the potentially significant task of facilitating the exchange of information between EU MS and UK post-Brexit.

Expected results	More efficient data processing is in place leading to optimisation of analytical work.
	Increased quality and completeness of Europol's intelligence picture allows for more effective response to MS operational cases and crisis situations.

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

Actions	Set up a SIRENE office[12] within Europol and develop relevant internal and external procedures for the information exchange and the processing of SIS II data for analytical purposes.
	Provide training on the SIS II and the newly acquired possibilities for Europol to all relevant Europol staff involved in data processing and analysis.
	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.
	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.
Expected results	Increased quality and completeness of Europol's intelligence picture with regards to SIS II alerts and through the exchange of supplementary information.

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

Actions	Maintain effective operational cooperation with the UK from the point the country ceases to be a Member State of the EU[13].

---

[12] 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.

[13] In compliance with the EU-UK Withdrawal Agreement (provided it enters into force).

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.

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.

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.

Exploit potential areas for collaboration stemming from the establishment of the European Union Agency for Asylum (ex. EASO).

Review the performance of the Brussels office in terms of efficiency.

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
Speed of first-line response to MS requests (days)	7.2	7
Accepted contributions to be processed	55,131	75,000
Operational Information Backlog (number of operational contributions pending processing)	2,702	1,500
% of total SIENA messages exchanged (by Europol) outside of office hours	9%	10%
Hit rate (Number of cross match reports and SIENA hit notifications per 100 accepted contributions)	9.2%	9%
Number of Mobile office deployments	306	400
SIENA messages exchanged by third parties (TP)	116,267	222,000
Operations supported by Europol involving cooperation partners	569	780
Operations supported by Europol involving private partners	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
Provision of Operational Support   o Handle ESOCC information; monitor information flows;   o Coordinate and support ESOCC operations;   o Perform ESOCC intelligence analysis and provide analytical support;   o 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;   o Support MS with operational capabilities and expertise that are not available widely at national level to enhance cost-effectiveness;   o Work closely with front-line investigators by providing on-the-spot, real-time information exchange and expertise (Mobile Forensic Kit, Mobile Office);   o Manage migrant smuggling-related operational information received from the guest officers deployed at the hotspots;   o 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);   o Provide testimony in court;

o Set up operational meetings and support Joint (EMPACT) Action Days.

Implementation of EU Policy Cycle priorities

o Support the EU Policy Cycle and increase its impact on the set priorities;
o Support the implementation of Multi-Annual Strategic Plans (MASP);
o Support the implementation of Operational Action Plans (OAP) to combat priority threats.

Strategy and Outreach

o Coordinate strategic intelligence collection and management;
o Provide dedicated strategic and tactical analysis support on SOC;
o Provide analytical contributions to improve the intelligence picture in different crime areas;
o Prepare and support prevention materials and campaigns;
o Develop expertise in the serious and organised crime mandated areas;
o Coordinate demand and development of new technical solutions;
o Coordinate R&D involvement;
o Organise major stakeholder events and conferences;
o Coordinate partnerships and stakeholder networks.

Operations - Commodities and Organised Crime Networks

Operations on Drugs

o Disrupt the Organised Crime Groups (OCGs) involved in cocaine trafficking and distribution (AP Cola);
o Disrupt the OCGs involved in heroin trafficking and distribution (AP Heroin);
o Disrupt the OCGs involved in synthetic drugs trafficking and distribution (AP Synergy);
o Disrupt the OCGs involved in Cannabis trafficking and distribution (AP Cannabis).

Operations on Top Organised Crime Groups

o Disrupt Mafia-structured OCGs originating in Italy and impacting other MS (AP ITOC);
o Disrupt Ethnic Albanian Organised Crime Networks (AP Copper);
o Disrupt Eastern European Organised Crime Networks (AP EEOC);
o Disrupt Outlaw Motorcycle Gangs (AP Monitor).

Operations on Weapons & Explosives

o Disrupt illicit trafficking in firearms and explosives (AP Weapons & Explosives).

Operations - Economic and Property Crime

Operations on Fraud

o Disrupt the capacity of OCGs and specialists involved in excise fraud (AP Smoke);
o Disrupt the capacity of OCGs and specialists involved in Missing Trader Intra Community fraud (AP MTIC);
o Disrupt the capacity of OCGs involved in fraud (AP Apate);
o Disrupt the capacity of OCGs and specialists involved in sport corruption (AP Sports corruption);
o Disrupt the capacity of OCGs involved in environmental crime (AP EnviCrime).

Operations on Counterfeiting

o 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);
o Disrupt the OCGs involved in Euro Counterfeiting (AP Soya);
o Manage the Intellectual Property Crime Coordination Coalition (IPC³) 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

intellectual property crime and, (iii) effective and efficient leverage of available resources, skills and capabilities of all stakeholders (AP Copy).

Operations on Property Crime

o   Combat organised property crime committed by Mobile Organised Crime Groups (AP Furtum).

European Migrant Smuggling Centre and Trafficking in Human Beings

Operations on Facilitation of Irregular Migration

o   Act as the EU Centre of expertise on migrant smuggling;
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);
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);
o   Monitor migration flows and their impact on crime; highlight links between migrant smuggling and other crime areas and terrorism;
o   Be the central Europol contact point in the EU Regional Taskforce (EU RTF).

Operations on Trafficking in Human Beings (THB)

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).

2019 Objectives

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

Actions	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).
	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.
	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.
	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.
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'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.

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[14].
	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.

---

[14] Toward a Bold Europol Response to Drugs in Europe (EDOC-#892562)

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 Apate 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.

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).

Increase cooperation with Frontex in the maritime domain in order to enhance the detection of environmental crime related to illegal fisheries and marine pollution.

Expected results	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.
	MS investigations in relation to fraud crime receive better and extended support.

A.3.6 Strengthen the fight against organised property crime.

Actions	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.
	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.
	Support the organisation of a Joint Action Day targeting various modalities of motor vehicle crime, including smuggling of stolen vehicles, and associated document fraud.
	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.
	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.
	Organise a Pickpocket Conference at Europol to discuss on-going operations, new modus operandi and prevention measures.
Expected results	Improved access to information and coordination of action in the EU in the area of organised property crime.
	MS investigations in relation to organised property crime receive better and extended support.

(* *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
Operations supported related to SOC	612	800
Operational reports delivered related to SOC	3,445	4,600
Satisfaction with operational support and analysis in the area of SOC	8.7	8.5
Number of cases where High Value Targets were identified	-	10
Operations supported by EMSC	134	130
On-the-spot support deployed related to EMSC (days)	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
Provision of Operational Support
o 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;   o 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;   o Support multidisciplinary cyber investigations and facilitate the secure information exchange with key public and private partners;

o Provide an on-the-spot service by deploying cyber analysts and/or specialists to support ongoing operations;
o 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).

Document Forensics

o Support MS investigations with regards to false documents, counterfeit currency and printing devices;
o Provide forensic services, reports and examinations, including forensics services accredited to ISO17020:2012;
o Support MS investigations with video enhancement analyses;
o Share the expertise and provide training in false document and currency identification;
o Support EU Policy Cycle priorities on document fraud and related investigations;
o Assist in the dismantling of clandestine print shops.

Digital Forensics

o 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;
o Provide technical support to MS investigations obstructed by encryption via the dedicated Decryption Platform;
o 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.);
o Provide support and guidance in relation to covert digital activities;
o Develop community of experts in the relevant digital forensic areas;
o Deliver the annual Digital Forensic Investigator training course.

Strategy and Outreach

o 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;
o Continually improve the management of EC3's growing network of external partners;
o Foster and facilitate the preparation and delivery of standardised prevention and awareness campaigns in relation to the cybercrime mandated areas;
o 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;
o Represent and promote the views of public safety and law enforcement agencies in the global discussion on Internet Governance;
o Coordinate and support the demand, development and delivery of comprehensive cybercrime training under the umbrella of a Training Governance Model at EU level;
o Collect, analyse and manage strategic intelligence, and further develop expertise with a view to supporting pro-active and innovative approaches;
o 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;
o Identify common challenges to combating cybercrime in collaboration with Eurojust;
o Coordinate the demand and development of new technical solutions and products, including R&D with the Forensic Experts Forum and other relevant stakeholders;
o Coordinate and provide advice to R&D priorities at national and EU level, particularly in relation to EU funding programs, if and where appropriate.

Thematic operations

Cyber Intelligence for Operations

o Collect information on cybercrime and cyber-facilitated crime threats and trends from a wide array of public, private and open sources;
o Support EU MS by identifying new modi operandi and identifying investigative opportunities through pro-active analysis and exploitation of the contributed data;
o Provide knowledge products with regard to technology and new criminal modi operandi online;
o Monitor new technological developments impacting cyber and traditional crimes and build expertise;
o Support EU MS with OSINT analysis and expertise;
o Provide operational, tactical and strategic support in the area of crypto-currency;
o 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

o Provide operational coordination and support to Member States' investigations in regard to cyber-dependent crimes of greatest concern (AP Cyborg);
o Focus on preventing and combating cyber criminality affecting critical infrastructure and network and information systems;
o 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;
o Provide a dedicated, secure and automated malware analysis platform to MS through the Europol Malware Analysis Solution (EMAS).

Operations on Child Sexual Exploitation

o Support the EU MS in preventing and combating all forms of criminality associated with the sexual exploitation of children (AP Twins);
o Tackle forms of criminal online behaviour against children, such as grooming, self-generated indecent material, sexual extortion and coercion, and web live streaming;
o 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;
o 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;
o 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;
o Deliver training courses on Victim Identification and Combating Online Sexual Exploitation of Children;
o Update regularly EU MS experts on intelligence relating to online platforms being set up, maintained or abused for the purpose of child sexual exploitation;
o 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

o 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);
o 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;
o 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);

o Execute the joint operational action against telecom fraud, in collaboration with law enforcement, judiciary and relevant private partners;
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.);
o Coordinate the detection, identification, dismantling, prosecution and prevention of money muling, together with key partners (Eurojust, financial sector, etc.);
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);
o Actively engage with priority regions to address payment fraud migration;
o Deliver the annual training course on Payment Card Fraud Forensics and Investigations.

Operations on Online Trade in Illicit Goods and Services

o Support the MS in combating criminal networks in regard to the administration and moderation of Dark Web related activities;
o Enhance the intelligence picture of the online trade in illicit goods and services online, in particular on the Dark Web;
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;
o Strengthen the operational coordination, de-confliction, prioritisation and investigation of Dark Web related crimes at an international level;
o Support the planning and execution of joint technical and investigative actions;
o Further develop knowledge and expertise on tools, tactics and techniques for conducting Dark Web investigations;
o Support the delivery of training related to Dark Web investigations.

J-CAT

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;
o Stimulate and facilitate the joint identification, prioritisation, preparation and initiation of cross-border investigations and operations by the J-CAT partners;
o Pro-actively drive intelligence-led, coordinated action against jointly identified, key cybercrime threats and top targets;
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;
o Facilitate the collaboration and operational engagement with Eurojust on cybercrime cases via the dedicated Eurojust cyber SNE;
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.

2019 Objectives

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.

Actions	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.*
	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.).*

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[15] 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)[16] 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.

---

[15] Subject to adoption of the Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment (COM/2017/0489 final)
[16] http://www.misp-project.org/

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	Create a second tier of decryption system in cooperation with the Joint Research Centre (JRC).
	Continuously monitor new trends in the use of encryption by criminals and explore different investigative opportunities and best practices in addressing the issue.
	Increase the cooperation with ENISA to identify, assess and define solutions to address the criminal abuse of encryption and online anonymity.
	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.
	Develop a Decryption Experts group with relevant stakeholders.
	Further develop Europol's capability for retrieving data from password protected mobile devices.
Expected results	Increased capacity and functionalities of Europol's Decryption platform.
	MS investigations receive better support and expertise with regards to the criminal abuse of encryption and online anonymity.
	Coordinated EU LEA strategy on tackling the criminal abuse of encryption and associated challenges.

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	Further engage with key cyber intelligence centres and cyber operational international taskforces (such as National Cyber-Forensics & Training Alliance, International Cyber Crime Operations Summit (ICCOS), etc.) in order to facilitate the alignment, de-confliction and operational cooperation. *
	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.
	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.*
	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.

	Organise a cyber exercise for EU LEA and key partners from the cyber security ecosystem to test the EU Law Enforcement Emergency Response Protocol.
	Actively participate in and support other pan-European/joint cyber exercises, focusing on the role of law enforcement.
	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.
	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.*
	Host the biennial expert meeting on technical investigations on printed devices.
	Explore possibilities for pro-active collaboration with key stakeholders on combating document fraud under the EMPACT document fraud priority.
Expected results	Improved joint operational activities with public and private partners of relevance.
	More effective levels of cooperation leading to better coordination and increased operational and strategic 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
Operations supported related to cybercrime	215	200
Operational reports produced related to cybercrime	662	1,000
Satisfaction with operational support and analysis in the area of cybercrime	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

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
Provision of Operational Support   o Coordinate criminal intelligence collection and management;   o Monitor law enforcement information flows on 24/7 basis;   o Manage CT-related operational information received from secondary security checks performed by the guest officer deployed at the hotspots;   o Perform in-depth analysis of CT information;   o Identify emerging threats and developments;   o Detect links between terrorism and organised crime in close cooperation with the other Europol centres;   o Provide operational support to MS in a wide range of terrorism-related areas and in the field of responding to a major terrorist crisis;   o Manage the CT JLT operational platform and the First Response Network;   o Support the deployments of Mobile office and other mobile toolkits;   o Provide technical/ forensic support on the spot;   o Provide support to court hearings;   o Organise operational meetings at Europol.
Thematic Operations   o 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);   o 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

offences associated with terrorism perpetrated by individuals, groups, networks or organisations who evoke Islam to justify their actions (AP Hydra);

o Prevent or combat terrorism by sharing analysis on related travel activities to terrorist hotspots, e.g. conflict zones and training venues (AP Travellers);

o 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).

Counter Terrorism Financing

o 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);

o Verify the link to terrorism in requests for data on financial payments;

o Support MS' investigations targeting networks facilitating the financing of terrorist actions or organisations;

o Provide support, including information on financial transactional data, to all operations where there is a link to terrorism;

o Liaise with Europol's Financial Intelligence Unit and with the competent ESOCC and EC3 units to close information gaps.

Strategy & Expertise

Strategy and Outreach

o 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;

o Contribute to specific ECTC developments such as improving connectivity of relevant systems and tools; closing the intelligence gap between terrorism and organised crime;

o 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;

o 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;

o Cooperate with EU institutions and agencies and international organisations on CT matters;

o Participate in and contribute to the work of the High-Level Commission Expert Group on radicalisation;

o 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;

o Perform the role of CT Program Board secretariat in assistance to its Chair;

o Organise stakeholder events, including the ECTC Advisory Group meetings and conferences on online terrorist propaganda.

Modus Operandi Monitor (MOM)

o Identify new terrorist Modi Operandi;

o Raise awareness on new Modi Operandi to all relevant partners;

o Provide tailored newsfeeds on terrorism trends and other relevant information by means of daily and monthly reporting to MS;

o Undertake joint actions with all relevant partners on preventive measures.

CBRN/E

o Manage and administer the Europol Platform for Experts pages:
 - EPE/EBDS (European Bomb Data System);
 - EPE/EEODN (European Ordnance Disposal Units Network);

o Ensure the permanent secretariat and the continuity of the activities of EEODN;

o Liaise with AP Weapons and Explosives to track possible new threats, trends and modus operandi involving CBRN materials and Explosives;

o Prepare strategic and technical reports on CBRN and Explosives;
o Deliver capacity-building initiatives for MS on CBRN and Explosives.

EU Internet Referral

Internet Monitoring and Referrals

o Perform scanning of social media and cyber environment, within the framework of prioritised areas (terrorism and illegal migration) or act upon MS' specific requests;
o Coordinate and share the identification tasks (flagging) of online terrorist and violent extremist content with a network of national counterparts;
o 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;
o Deliver operational and strategic products;
o 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;
o Organise and coordinate Targeted Referral Joint Action Days in cooperation with experts from MS and online service providers (OSPs);
o Build a network of academics and researchers in terrorism, radicalisation, computer sciences, information technologies, social network analysis and other pertinent areas of social science.

Internet Investigation Support

o Deliver operational and strategic products;
o Provide operational support and support coordination of CT Internet-based investigations;
o Organise operational meetings;
o Support MS in connecting with online service providers and analysing the digital footprint of a target in CT investigations through the SIRIUS capability.

Technical Support and R&D

o Provide technical support to the Referrals and Operations teams;
o Provide expertise on big data management and analysis to the ECTC;
o Establish a European centre of excellence, by strategically enhancing partnerships with cooperation partners and investing resources in Research & Development;
o Act as an Innovation Hub for Europol and the EU MS in the field of counter-terrorism;
o Contribute to the Innovation work-stream within the Operations Directorate by investing on prototyping initiatives;
o Develop the SIRIUS Platform to support Internet-based investigations and cross border access to e-evidence;
o Develop projects together with the private sector and academia on new techniques and tools in the context of EU grant funding programmes.

2019 Objectives

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.

Actions	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.

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[17]. 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[18], 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[19] 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.

---

[17] EU Action Plan to strengthen chemical, biological, radiological and nuclear (CBRN) security, Oct 2017
[18] Subject to appropriate legal basis in place, i.e. international agreements or working arrangements
[19] 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)

<table>
<tr><td colspan="2">A.5.2. Expand the scope of the Cross Border Access to Electronic Evidence (SIRIUS) Project.[20]</td></tr>
</table>

Actions	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.*
	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.
	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.
	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.
	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.*
	Increase SIRIUS's geographical scope by introducing guidelines on requesting data from OSPs based in countries other than the US.*
	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.
Expected results	Improved Europol's capabilities in the area of digital cross border investigations which leads to better and extended support to MS.
	Increased MS capacity to prepare effective digital data requests to OSPs and obtain electronic evidence.

<table>
<tr><td colspan="2">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.</td></tr>
</table>

Actions	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.*
	Support Internet companies by providing expertise on the development of and training in new content detection and identification technology.
	Develop and test tools that allow for the detection of terrorist content across platforms.*

---

[20] Subject to receiving a grant from the European Commission and agreement on concrete priorities to be pursued by the SIRIUS project.

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 [21] 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[22] 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.

A.5.4. Implement the affiliation of the ATLAS Network of Special Intervention Units within the structure of Europol.*	
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.

---

[21] Subject to adoption of draft Regulation on preventing the dissemination of terrorist content online, COM(2018) 640 final.
[22] 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
Operations supported related to CT	469	500
Operational reports produced related to CT	1,358	1,700
Satisfaction with operational support and analysis in the area of CT	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
SIENA messages exchanged by CT units	41,580	55,000
Number of accepted contributions related to CT	4,845	7,000
Number of EIS objects related to CT	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%
% of successful referrals by the EU IRU of suspicious internet content related to terrorism and violent extremism	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
o   Establish and implement a common, consistent and holistic approach towards strategic analysis across the Operations Directorate;   o   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

- Joint EMCDDA-Europol European Drug Markets Report
- 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

o Deliver thematic intelligence analysis products within the areas of serious and organised crime, cybercrime and terrorism;
o Deliver open source monitoring reports based on the business need;
o Organise the meetings of Advisory Groups (SOCTA, TE-SAT, best practices of analysis, etc.).

Analysis & Training Coordination

o Oversee the development, implementation and maintenance of efficient operational information management processes;
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;
o Ensure compliance with the data protection regulation and mitigate the risk of misconducts of sensitive data usage;
o Coordinate Europol's training initiatives and respond to any new training needs of MS which may arise (incl. joint Europol/CEPOL training);
o Coordinate and deliver training to operational staff.

Strategic Intelligence - direct support

Special Tactics

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;
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;
o Manage EU Most Wanted List containing high-profile internationally-wanted criminals;
o Manage the High Risk Informant Database (HRDB) - a coded database allowing a more accurate risk assessment when working with foreign informants;
o Manage the European Tracking Solution (ETS);
o Manage the Virtual Command Post tool for live information exchange during operations;
o Support the implementation of MASP and OAP through the involvement in joint investigations, large-scale operations and/or joint action days;
o Organise strategic expert meetings, training, awareness raising and prevention activities in the area of knowledge management and in support of specialist networks.

EMPACT Support

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);
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;
o Monitor and report on the EMPACT projects' progress. Provide recommendations;
o Coordinate the planning of Joint Action Days;
o Facilitate communication and collaboration between the crime priorities having common goals and/or interdependencies.

Passenger Name Records (PNR)

o Implement Europol's role in the EU PNR architecture in line with the EU Directive;
o Utilise effectively PNR data exchange provisions;
o Provide support to the connectivity and data exchange among the Passenger Information Units (PIUs) in MS;

o Provide support to PNR related projects;
o Participate in the informal working group on PNR.

Deployment Management and Support

o Manage and support large scale deployments by Europol, as well as deployments linked to first responses requested by MS;
o Coordinate, manage and support the guest officer deployments.

Financial Intelligence

o Process and handle financial intelligence information;
o Provide financial intelligence and operational support to MS and TP within the areas of money laundering, asset recovery, terrorism financing and corruption;
o Provide financial intelligence to the ESOCC, EC3 and the ECTC;
o Provide financial intelligence and operational support to EMPACT related activities;
o Support corruption investigations initiated by MS and promote the use of SIENA for the information exchange between anti-corruption authorities;
o Provide operational support on the spot, including for Joint Action Days (e.g. mobile office deployments);
o Manage and support the development of the FIU.net computer network;
o Organise the FIU.net Advisory Group meetings and dedicated workshops based on the Service Level Agreement (SLA);
o Organise on-site trainings on the FIU.net based on the SLA;
o Manage all EPEs relating to financial intelligence (FCIC, ALEFA, AMON, CARIN, EFIPPP, FIU net and FIU net AG) and handle their growth;
o 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 terroris financing in the framework of the Expert group on Money Laundering and Terrorist Financing;
o Co-chair with the European Commission the ARO platform meetings;
o Support projects related to the fields of financial intelligence, money laundering, asset recovery, terrorism financing and/or corruption;
o Support and host the secretariats for the Anti-Money Laundering Operational Network (AMON) and the Camden Asset Recovery Inter-Agency Network (CARIN);
o Support the triparty Working Group on digital currencies (co-host secretariat jointly with Interpol and the Basel Institute);
o 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;
o Develop, promote and support the Europol Financial Intelligence Public Private Partnership;
o Contribute to policy development such as guidance drafting and standards revision when requested by the Commission;
o Collect EU MS requirements; prioritise and deliver strategic products.

2019 Objectives

A.6.1. Contribute to the development of a common EU view on criminal analysis.

Actions	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.
	Develop in cooperation with MS common standards for analysis training.

	Prepare the curriculum for and organise a Europol Summer School on criminal analysis.*
	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.
	Provide technical advice on initiatives related to preparation of EU legislation on crime analysis, if any.
Expected results	Improved cooperation in the EU based on the agreed common view and standards on analysis leading to an increased operational impact.
	MS investigations receive better and extended analytical support.

A.6.2. Strengthen Europol's capabilities to deliver quality strategic reports.	
Actions	Ensure having in place up-to-date methodologies for each type of strategic analysis reports and their cross-organizational application.
	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.
	Further develop the concept of conducting strategic analysis by setting up joint analysis teams with MS analysts.
	Identify training needs and offer the necessary training opportunities for Europol's strategic analysts.*
	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.
	Make full use of the opportunities of the newly available travel information for the strategic and thematic purposes.
	Produce the mid-term review of new, changing or emerging threats paying particular attention to the EU crime priorities defined in 2017.
Expected results	Provision of timely and authoritative strategic intelligence products to MS on current criminal phenomena.
	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.

A.6.3. Develop Europol's capabilities in the area of travel intelligence in line with the Travel intelligence Roadmap.*	
Actions	Further develop and deliver specialised operational analysis reports on the basis of travel information and intelligence stemming from PNR and Advance Passenger Information (API).*

Further develop and deliver strategic products reflecting crime specific characteristics concerning travel movements as input for the definition of targeting rules.*

Support the development of innovative and interoperable solutions to meet the business requirements of the travel intelligence community.

Create and gradually extend a dedicated liaison network with direct connection with relevant travel intelligence entities in the MS and other partnering countries.

Organise a Travel Intelligence conference.

Enhance cooperation with private partners relevant for the collection of travel intelligence.*

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.*

Arrange for the possible acquisition of the database on suspicious travel agencies of the International Air Transport Association (IATA).

Expected results	Increased quality and completeness of Europol's intelligence picture with regards to travel information.
	MS investigations receive the required support for the processing of travel data and the results of such processing through Europol's operational products.

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

Actions	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.
	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.
	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.
	Further develop a tool for de-conflicting online undercover operations.
	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.*

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/functionalities 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.

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[23] creating a network of counter-terrorism financing experts and improving cooperation with private sector on CT matters.*

Support the EBOCS project[24] 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

---

[23] The BeCaNet Project is the 'best practice, capacity building and networking initiative among public and private actors against Terrorism Financing', led by BKA, Germany.
[24] 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
Operations supported with Financial Intelligence products/services	146	150
Number of operational reports related to Financial Intelligence	790	950
Satisfaction with operational support and analysis in the area of Financial Intelligence	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.

Internal Control Coordination

o   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);
o   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;
o   Maintain Europol's ethics package;
o   Implement the Internal Control Framework, including the maintenance of the financial model of Europol (appointment decisions, etc.);
o   Monitor the Internal Control System based on a dedicated list of internal control indicators with a view to assessing its effectiveness;
o   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.

Corporate communications

Manage open sources

o   Provide access to, user support and training on the use of Open Source tools and databases. Organise the Europol Open Sources Intelligence Conference;
o   Manage European Media Monitoring tool; deliver effective media monitoring, crisis monitoring and media impact products and services;
o   Manage digital subscriptions and periodicals.

Internal communication

o   Maintain and develop Europol's intranet as the main internal communication tool;
o   Organise staff and managerial events.

Public relations

o   Maintain media, press and public relations;
o   Deliver annual and ad hoc media impact reports after events or operations;
o   Support high level visits and organise high level events such as the European Police Chiefs Convention (EPCC);
o   Coordinate external publications;
o   Provide corporate audio-visual productions;
o   Organise awareness-raising activities in Member States and Third Countries;
o   Organise media training for Europol staff and annual photo competition.

Corporate services

Coordinate Europol participation in MB, MB Working Groups and follow up to MB decisions.

Corporate planning, monitoring and reporting

o   Prepare the Europol Strategy on particular intervals and related multi-annual business planning documents;
o   Prepare the annual business planning documents;
o   Prepare quarterly, bi-annual and annual corporate performance reporting;
o   Support and conduct internal and external stakeholder surveys and evaluations;
o   Coordinate Europol's involvement in EU grant funded projects.

Corporate content management

o   Coordinate corporate document and records management incl. archiving;
o   Provide end user support and training for information management systems and services;
o   Deliver process analysis, improvement and facilitation services;
o   Ensure that all processes and protocols for new initiatives are in place to guarantee the methodological consistency of the work;
o   Deliver training on quality and process management.

Legal services – Commercial law

o Develop and maintain Europol's legal framework for finance, procurement, grants and facilities;
o Advise on existing contract interpretation and escalation;
o Advise on litigation arising out of tender procedures and/or contracts;
o Review Europol's participation in grant funded projects and awarding of grants;
o Handle contract related complaints to the European Ombudsman;
o Deliver internal training on legal procurement, low value contracts, contract management and legal issues in evaluation of tenders.

Legal services – Employment law

o Develop and maintain HR legal framework and implementing rules to the EU Staff Regulations;
o Provide legal advice concerning staff and HR related questions;
o Handle staff related complaints and requests including court cases to the European Ombudsman and the Court of Justice of the EU;
o Participate in lawyers' networks (EU IALN and international networks) and perform assessments following requests by IALN.

Procurement

o Coordinate tender planning in line with annual business and budget planning;
o Manage and supervise tender procedures;
o Continuously update procurement related implementing rules, policies, guidelines, documents, tender processes, tender model documentation, etc.;
o Deliver internal training on tenders;
o Participate in Network Agencies Procurement (NAPO) and exchange best practices on contract database and contract management.

Security

Physical Security

o Ensure security of Europol staff, building and installations in compliance with European standards on operational security;
o Maintain close cooperation with relevant networks and other agencies; take part in peer reviews; attend conferences/ masterclasses on Safety & Security;
o Provide training for security officers;
o Provide internal first aid, emergency response and evacuation training for staff;
o Deliver risk assessments related to Europol and its staff (e.g. for business trips).

Confidentiality & Information Security

o Ensure timely accreditation of information systems;
o Perform regular risk assessment of systems prior to becoming operational as well as compliance audits;
o Organise security awareness events and training for staff;
o Update information security policies;
o Regularly report to the Security Coordinator and the Security Committee;
o Handle requests for handling higher classified information;
o Handle clearance requests;
o Participate in EU security networks, international security forums or meetings organised by the Council Security Office.

Internal Investigation Service

o Participate in the pool of internal investigators (as required by the Commission);
o Implement the Europol Anti-Fraud Strategy.

Security Engineering

o Provide on-call assistance for technical security installations;
o Adjust, finalise and implement all technical security installations;
o Implement changes of security requirements in infrastructure.

Business Continuity

o Analyse, design, develop and implement the business continuity framework;
o Coordinate Europol's overall crisis management capability incl. organising an annual crisis management exercise for the Crisis Management Team;
o Coordinate Disaster Recovery activities.

Personal Protection

o Execute protective security operations for the Executive Director and staff;
o Coordinate and provide security in high level meetings and media events;
o Transport classified documents;
o Maintain tactical personal protection equipment and related security installations;
o Participate in the relevant European networks related to protection of public figures, personal protection services and threat assessment; support the related EPE.

Administration

Resource planning and reporting

o Establishment of the budget and staff establishment plan;
o Monitor the implementation of the budget and the staff establishment plan at corporate level;
o Report on Europol's financial and human resources to different stakeholders;
o Monitor activity based management;
o Manage the Financial Management System (ABAC).

Human Resource Management

o Develop and update HR related strategy, implementing rules, policies, guidelines, processes and templates;
o Organise the recruitment and selection of staff and SNEs;Follow up internal mobility;
o Plan and administer internships;
o Provide administrative support to Guest Officer deployments and to operational grants;
o Manage staff contracts and personal files;
o Manage ECAS accounts;
o Determine rights and entitlements of Europol staff, local staff and SNE's;
o Manage the salary administration;
o Administer working conditions and working hours of staff, as well as annual, medical and special leave;
o 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;
o Represent Europol in the Advisory Board of the European School;
o Deliver health and wellbeing-related services;
o Implement actions in view of creating a corporate culture of diversity;
o Organise pre-employment and annual medical checks;
o Coordinate training of staff;
o Coordinate the appraisal and reclassification processes;
o Deliver pension advice;
o Manage the HR Management System and the Travel Management System.

Budget administration

o Develop and update finance related strategy, implementing rules, policies, guidelines, processes and templates;
o Execute financial initiation of revenue and expenditure;
o Perform ex-ante and ex-post financial verification of all financial operations;
o Manage the travel budget and refund of taxes.

Facilities Management

o Develop and update facilities-related strategy, implementing rules, policies, guidelines, processes and templates;

o   Manage the facilities-related budget;
o   Manage facilities-related contracts including the building insurance contracts;
o   Manage the building(s), including housing, lease and service level agreements with the Host State as well as building related programmes;
o   Manage the sites abroad, inclusive service level agreements, with the involved agencies and governmental institutes;
o   Manage the non-ICT assets;
o   Ensure an efficient space allocation in the building(s);
o   Deliver meeting and conference services;
o   Deliver travel management services;
o   Coordinate translations with the Translation Centre For the Bodies of the EU (CdT);
o   Manage and improve the Facilities Management Information System, Online Registration Tool and Conference Booking Tool.

ICT administrative support

Infrastructure Services

o   IT Operations Centre: support and monitor all Europol IT Applications and Infrastructure;
o   Define and maintain the technical profile and resource list;
o   Periodically assess the need for profiles and technical skills;
o   Run and maintain all non-ICT aspects of the Europol Datacentres.

Customer Service Centre

o   Deliver Helpdesk services to external customers (MS and partners) and staff;
o   Define and implement the request management process to handle all incoming requests from both customers and staff;
o   Define and maintain MoU's for MS and partners.

Workplace Services

o   Order, deploy and maintain end-user hardware and software;
o   Periodic and urgent software and operating system patching of user-related hardware.

ICT Financial & Contract Coordination

o   Integrated ICT planning, financial management and financial administration;
o   Supplier, license and asset management;
o   Tender and procurement planning for ICT;
o   ICT contract management.

2019 Objectives

A.7.1. Continue optimising Europol's corporate functions.

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

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.

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	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.
	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.
	Deliver the functional and technical requirements and tender the design for a new additional permanent building to provide for a long term housing solution.
	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.
	Finalise the upgrade of the audio-video installation in the conference environment.
	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.
	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.
	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.
Expected results	Existing workspace and new office locations are used in an optimal way to accommodate organisational growth.
	Europol is better equipped to handle increasing demand for ICT services.

A.7.3. Establish a new strategy [25] for effective awareness raising on Europol's products and services to law enforcement stakeholders.

Actions	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.).
	Organise consultation with trainers of the police academies of MS competent authorities to identify possibilities to

[25] Provisional name until the document is finalised and agreed in 2019.

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.

Liaise with the Heads of the Liaison Bureaux and exchange/discuss ideas regarding the joint approach to raise awareness of international cooperation.

Approach CEPOL with regards to establishing synergies with CEPOL's webinar programme.

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%
Commitment Rate Europol Budget	84.7%	≥ 95%
Payment Rate Europol Budget	62.7%	≥ 90%
Budget Outturn rate	-	≤ 2%
% Late Payments	13%	≤ 5%
Vacancy rate	3.6%	≤ 2%
Sickness rate	-	≤ 3.5%
Turnover rate	4.5%	10%
% of pending critical/very important audit recommendations implemented within the agreed deadline with the auditing body	71%	85%
% of Work Programme objectives implementation	-	80%
% Staff Engagement (via Staff Survey)	-	65%
% Satisfaction with Europol's image (via User Survey)	-	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:

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

o   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.);
o   Provide consultation in relation to legal and technical-organisational data protection safeguards;
o   Provide training and awareness program for staff handling personal data;
o   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:

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

o   Support the coordination of the MB's work and ensure its coherence;
o   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;
o   Provide the MB with the administrative support;
o   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.

ANNEXES

Annex I: Resource allocation per Activity 2019-2021

Annex II:

      A. Human and Financial Resources 2019-2021

         Table 1 – Expenditure

         Table 2 – Revenue

         Table 3 – Budget outturn and cancellation of appropriations

      B. Draft Estimate of Revenue and Expenditure 2019

Annex III:

         Table 1 – Staff population and its evolution; Overview of all categories of staff

         Table 2 – Multi-annual staff policy plan year 2019–2021

Annex IV:

      A. Recruitment policy

      B. Appraisal of performance and reclassification/promotions

      Table 1 - Reclassification of temporary staff/promotion of officials

      Table 2 - Reclassification of contract staff

      C. Mobility policy

      D. Gender and geographical balance

      E. Schooling

Annex V: Buildings

Annex VI: Privileges and immunities

Annex VII: Evaluations

Annex VIII: Risks 2019

Annex IX: Procurement plan 2019

Annex X: Grants 2019

Annex XI: Organisation chart

Annex I: Resource allocation per Activity 2019-2021

	Budget 2019				Forecast 2020		Forecast 2021	
	Number of staff (TA,CA,SNE) [26]	% of total staff	Budget allocation[27] €	% of total budget	Number of staff	Budget allocation €	Number of staff	Budget allocation €
A.1. Development of operational systems	146	16%	38,269,000	28%	173	41,844,300	185	43,952,743
A.2. Information Hub	74	8%	10,816,000	8%	69	11,783,349	70	12,031,183
A.3. Combating Serious Organised Crime	137	15%	23,786,000	17%	146	19,561,230	151	20,406,842
A.4. Combating Cyber Crime	92	10%	12,021,000	9%	101	12,677,504	105	13,454,279
A.5. Counter Terrorism	111	12%	12,180,000	9%	116	13,026,655	120	13,741,922
A.6. Provision of cross-cutting operational capabilities	75	8%	8,884,000	6%	78	14,871,147	80	15,279,858
A.7. Governance, support and administration	241	27%	29,438,458	21%	236	29,574,981	239	30,326,411
Independent functions: Data Protection Function Internal Audit Capability Management Board Accountancy Unit	18	2%	2,911,000	2%	17	2,792,834	17	2,820,762
TOTAL	**894**	**100%**	**138,305,458**	**100%**	**936**	**146,132,000**	**967**	**152,014,000**

---

[26] The allocation of the posts in 2019 is preliminary at this stage. Final allocation of the posts in 2019 is pending on the outcome of the reorganization proposal to be presented to the Management Board in February 2019.
[27] incl. salary.

Annex II:

A. Human and Financial Resources 2019 – 2021

Table 1: Expenditure

Expenditure (Only C1 fund source)	Commitment / Payment appropriations			
	2018	**2019**	**2020**	**2021**
Title 1 Staff Expenditure	79,421,520	84,205,258	93,115,000	98,468,000
Title 2 Other Administrative Expenditure	12,805,100	14,095,700	13,792,000	13,929,000
Title 3 Operational Activities	38,018,900	40,004,500	39,225,000	39,617,000
Total expenditure	**130,245,520**	**138,305,458**	**146,132,000**	**152,014,000**

Table 2 – Revenue

REVENUES (only IC1)	Executed Budget 2017	Budget 2018	Budget 2019	VAR 2019/ 2018
1 REVENUE FROM FEES AND CHARGES		P.M.	P.M.	
2. EU CONTRIBUTION	**114,623,613**	**130,245,520**	**138,305,458**	**1.06**
Of which assigned revenues deriving from previous years' surpluses	2,669,000	1,868,000	1,158,000	
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)	**-**	P.M.	P.M.	**-**
4 OTHER CONTRIBUTIONS	**-**	P.M.	P.M.	**-**
5 ADMINISTRATIVE OPERATIONS	**-**	P.M.	P.M.	**-**
Of which interest generated by funds paid by the Commission by way of the EU contribution(FFR Art. 58)	-	P.M.	P.M.	**-**
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT	-	P.M.	P.M.	**-**
7 CORRECTION OF BUDGETARY IMBALANCES	-	P.M.	P.M.	**-**
TOTAL REVENUES	**114,623,613**	**130,245,520**	**138,305,458**	**1.06**

Table 3 – Budget Outturn Cancellation of appropriations

Calculation Budget Outturn

BUDGET OUTTURN	2015	2016	2017
Revenue actually received (+)	88,516,920	117,390,869	119,696,212
Payments made (-)	-74,639,953	-102,836,986	-110,402,762
Carry-over of appropriations (-)	-15,131,537	-18,977,641	-18,756,290
Cancellation of appropriations carried over (+)	3,563,930	1,612,811	834,972
Adjustment for carry-over of assigned revenue appropriations from previous year (+)	360,829	4,677,757	9,783,165
Exchange rate differences (+/-)	-1,318	1,439	3,595
Total	**2,668,872**	**1,868,249**	**1,158,893**

Budget Outturn

The overall draft budgetary outturn for the financial year 2017 comes to almost € 1.2M. This includes the following:

- An amount of € 320K of the 2017 budget was not committed and lapsed. The majority of the unused budget is within Operations (Chapter 30). This includes an amount of € 177K for EMPACT grants which remained unspent due to limited number of applications;

- An amount of € 835K of appropriations carried forward from 2016 to 2017 was not used;

- The exchange rate difference was € 3.6K (gain).

Cancelation of payment appropriations carried forward

The carry forward to 2017 came to a total of € 9.2M to cover existing commitments. The majority of this was carried forward from commitments taken under fund source C1 (€ 8.98M, representing 9% of the 2016 budget). An amount of € 219K was carried forward from the appropriations arising from internal assigned revenue (fund source C4 and C5).

The final implementation rate of the carry forward was 90.9% at the end of the year, which is 6.4% higher than in 2016. A total of € 835K was not used and is thus incorporated in the final budget outturn. Out of the € 835M not used:

- € 59K relates to Title 1, which is 10% of the carried forward under Title 1 (€ 590K);
- € 125K relates to Title 2, which is 3.4% of the carried forward under Title 2 (€ 3.66M);
- € 651K relates to Title 3, which is 13.2% of the carried forward under Title 3 (€ 4.95M).

Unused amounts related to:

- An amount of € 126K remained unspent for travel expenses after the final correction of the closure of the first grant for security checks at Hotspots;
- An amount of € 379K for various ICT consultancies and € 71K for other SW and HW related expenditure;
- An amount of € 57K for fixed telephone costs and € 22K for internet and mobile telecom costs;
- An amount of € 84K for various administrative and governance expenditure;
- An amount of € 60K for various operational expenditure; and
- An amount of € 35K for various facilities related expenditure.

Annex II:

B. Final Budget 2019[28]

Final Budget 2019	Budget Outturn 2017	Budget 2018	Budget 2019	VAR 2019/ 2018
Title 1 Staff Expenditure	**71,864,946**	**80,974,455**	**84,205,258**	**1.04**
11 Salaries & allowances	67,051,198	75,210,554	77,816,418	1.03
- of which establishment plan posts	57,399,939	64,196,005	65,876,418	1.03
- of which external personnel	9,651,260	11,014,549	11,940,000	1.08
13 Sociomedical infrastructure	934,138	1,045,698	1,239,000	1.18
14 Training	330,976	353,781	150,000	0.42
15 Other staff-related expenditure	3,468,959	4,286,581	4,903,840	1.14
16 Entertainment and representation expenses	79,674	77,842	96,000	1.23
Title 2 Other administrative expenditure	**9,782,622**	**10,826,923**	**14,095,700**	**1.30**
20 Rental of buildings and associated costs	5,716,491	7,047,680	9,039,000	1.28
21 Information and communication technology	1,697,421	1,503,735	1,784,000	1.19
22 Movable property and associated costs	734,914	794,381	1,414,000	1.78
23 Current administrative expenditure	337,512	210,472	428,700	2.04
24 Postal charges and telecommunications	633,567	703,256	830,000	1.18
25 Statutory expenditure	662,719	567,400	600,000	1.06
Title 3 Operational activities	**32,655,720**	**38,444,142**	**40,004,500**	**1.04**
30 Operations	8,472,018	12,824,786	14,878,500	1.16
31 Operational information technology	19,537,342	15,486,662	19,386,000	1.25
32 Telecommunication costs for operational activities	881,794	918,693	1,350,000	1.47
33 Seconded National Experts (Operational)	3,386,066	3,855,000	4,000,000	1.04
34 EPCC	268,500	269,000	300,000	1.12
35 Heads of Europol National Units	110,000	90,000	90,000	1.00
38 Decryption Platform		5,000,000	-	-
TOTAL EXPENDITURE	**114,303,288**	**130,245,520**	**138,305,458**	**1.06**

Quarterly estimate of cash payments and receipts:

Chapter	RECEIPTS	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	Total 2019
90	Regular subsidy from the Community	34,576,365	34,576,365	34,576,365	34,576,365	138,305,458
	Total Receipts	**34,576,365**	**34,576,365**	**34,576,365**	**34,576,365**	**138,305,458**

Title	PAYMENTS	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	Total 2019
1	Staff in active employment	20,840,801	20,840,801	20,840,801	20,840,801	83,363,205
2	Other administrative expenditure	2,466,748	2,466,748	2,466,748	2,466,748	9,866,990
3	Operational activities	8,000,900	8,000,900	8,000,900	8,000,900	32,003,600
	Total Payments	**31,308,449**	**31,308,449**	**31,308,449**	**31,308,449**	**125,233,795**

	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter
Receipts - Payments	3,267,916	3,267,916	3,267,916	3,267,916
Cumulative	3,267,916	6,535,831	9,803,747	13,071,663

---

[28] Figures are rounded so the sum of the individual amounts may differ from the totals.

Annex III:

Table 1 – Staff population and its evolution; Overview of all categories of staff

Staff population [1]		Actually filled as of 31.12.2016 [2]	Authorised under EU Budget 2017 [3]	Actually filled as of 31.12.2017 [4]	Authorised under EU budget for year 2018 [5]	Final Budget 2019	Draft Budget 2020 [6]	Envisaged in 2021 [7]
TA	AD	476	517	521	544	559	624	655
	AST	29	33	29	32	32	32	32
	AST /SC	0	0	0	0	0	0	0
TOTAL TA [8]		**505**	**550**	**550**	**576**	**591**	**656**	**687**
CA GF IV		30.41	43	34.66	55	52	55	55
CA GF III		70.02	82	86.06	113	118	110	110
CA GF II		32.50	40	32.50	44	62	44	44
CA GF I								
TOTAL CA [9]		**132.93**	**165**	**153.22**	**212**	**232**	**209**	**209**
SNE [10]		**64.2**	**71**	**65.45**	**71**	**71**	**71**	**71**
Structural service providers [11]		31	50	41	50	50	50	50
TOTAL		**733.13**	**836**	**810**	**909**	**944**	**986**	**1017**
External staff[12] for occasional replacement[13]		9.33	10					

[1]This table provides all staff categories at Europol except trainees and Europol Liaison Officers. At the end of 2017 there were 32 trainees and around 220 Europol Liaison Officers

[2] The figures below include 42 TA posts (all in AD function group) that were not filled on 31.12.2016 but for which recruitment procedures were finalised and offer letters sent to selected candidates

[3] As authorised for officials and temporary agents (TA) and as estimated for contract agents (CA) and seconded national experts (SNE)

[4] The figures below include 15 TA posts (all in AD function group) that were not filled on 31.12.2017 but for which recruitment procedures were finalised and offer letters were sent to selected candidates

[5] As authorised for officials and temporary agents (TA) and as estimated for contract agents (CA) and seconded national experts (SNE)

[6] Tabular explanation of the effects on staff population is provided on the page below

[7] Ibid

[8] Headcounts

[9] FTE (annual averages)

[10] FTE (annual averages). The figure reported as of 31.12.2017 excludes FTE for SNE Guest Officers (30.78)

[11] FTE (annual averages)

[12] FTE (annual averages)

[13] Annual average FTE of CA's covering TA's on maternity leave, long-term sick leave and TA's working part-time. As these staff concern CAs the figure is from 2017 onwards fully integrated in the line for TOTAL CA.

Annex III: Table 2 - Multi-annual staff policy plan 2019-2021

Category and grade	Establishment plan in EU Budget 2017	Filled as of 31/12/2017	Modifications in year 2017 in application of flexibility rule [1]	Establishment plan in voted EU Budget 2018	Modifications in year 2018 in application of flexibility rule [2] [3]	Establishment plan in voted EU Budget 2019	Establishment plan in Draft Budget 2020	Establishment plan 2021
	TA only	TA only	TA only	TA only	TA only	TA only	TA only	TA only
AD 16								
AD 15	1	1	1	1	1	1	1	1
AD 14	1	1	1	1	1	1	2	2
AD 13	5	2	5	5	5	5	6	7
AD 12	11	6	11	11	11	11	13	14
AD 11	17	11	17	17	17	16	19	21
AD 10	30	10	30	28	28	23	35	38
AD 9	61	37	61	61	61	61	70	75
AD 8	97	75	97	100	90	89	99	104
AD 7	126	119	126	128	132	132	154	164
AD 6	139	247	139	158	177	192	208	214
AD 5	29	12	29	36	21	28	17	15
Total AD	**517**	**521**	**517**	**546**	**544**	**559**	**624**	**655**
AST 11	0	0	0	0	0	0	0	0
AST 10	0	0	0	0	0	0	0	0
AST 9	0	0	0	0	0	0	0	1
AST 8	2	0	2	3	3	0	5	4
AST 7	5	3	5	5	5	5	4	5
AST 6	6	4	6	6	6	6	7	7
AST 5	8	7	8	7	7	7	7	7
AST 4	8	10	8	5	8	8	6	5
AST 3	3	1	3	3	1	3	2	2
AST 2	1	4	1	1	2	3	1	1
AST 1	0	0	0	0	0	0	0	0
Total AST	**33**	**29**	**33**	**30**	**32**	**32**	**32**	**32**
AST/SC6	0	0	0	0	0	0	0	0
AST/SC5	0	0	0	0	0	0	0	0
AST/SC4	0	0	0	0	0	0	0	0
AST/SC3	0	0	0	0	0	0	0	0
AST/SC2	0	0	0	0	0	0	0	0
AST/SC1	0	0	0	0	0	0	0	0
Total AST/SC	**0**	**0**	**0**	0	0	**0**	**0**	**0**
TOTAL	**550**	**550**	**550**	**576**	**576**	**591**	**656**	**687**

[1] In line with Article 38(1) of the framework Financial Regulation, the management board may modify, under certain conditions, the establishment plan by in principle up to 10% TA only of posts authorised, unless the financial rules of the body concerned allows for a different % rate.
[2] Ibid
[3] Net modification and explanations for the modifications are provided on the page below

Explanations on the modifications and changes in relation to the establishment plans from 2019 to 2021

Modification to 2018 establishment plan using the flexibility contained with Article 38(1) of framework Financial Regulation.

The modifications envisaged to the establishment plan 2018 can be summarised as follows:

Modification	Budgetary effect
4 AD8 downgraded to AD7	Savings
6 AD8 downgraded to AD6	Savings
13 AD5 converted to AD6	Increase
2 AD5 downgraded to AST4	Savings
1 AST3 converted to AST4	Increase
1 AST3 downgraded to AST2	Savings

In total the modifications involve 54 post movements which constitute around 9% of the total number of 576 established posts within the allowable 10% contained within Article 38 and expenditure impact of the total changes results in budget savings.

The staff turnover was 7.6% at the end of 2017 which is considerably lower than last year (14.2%). This difference can be partly explained by the number of staff for whom the second contract was ending in 2017 (fewer compared to 2016).

Replacement of staff occurs in many instances at entry level thus reducing the grade of many posts of long-serving staff. The modified establishment plan 2018 provides a more accurate reflection of the organisation in terms of actual grades allocated to staff and current and upcoming vacancies, taking into account the following factors:

- 38 staff members left Europol during 2017 with most of them being replaced or due to be replaced in lower grades;
- Similar profiles are replaced in entry grades, i.e. in most cases lower than those of leaving staff;
- In many cases when post profiles are reviewed and updated they are converted into lower level posts (e.g. Senior Specialist/Senior Analyst into Specialist/Analyst).

Reclassification adjustments in the Establishment plans for 2019, 2020 and 2021

Europol implements reclassification on an annual basis. The establishment plans for 2018 to 2021 not only reflect the changes required in relation to new staff allocations but also changes to facilitate the reclassification process and potential changes to staff grades. At the end of the reclassification 2016 4% of staff (temporary agents) was reclassified. For future years depending on the grades the establishment plan foresees approximately 10% reclassification.

Annex IV:

A. Recruitment policy

Europol follows the Staff Regulations of Officials of the European Communities (ECSR) and Conditions of employment of other servants of the European Communities (CEOS)[29]. Europol's recruitment procedure is independent from that of other EU institutions and agencies. It has no permanent officials, but is staffed by Temporary Agents and Contract Agents recruited through open selection procedures.

Europol has adopted implementing provisions for the use and engagement of both Temporary and Contract Agents and conducts its recruitment procedures. The current process is currently being reviewed in light of the preliminary adoption by the MB of the TA2f provisions (art 56 CEOS-EUSR).

Key functions	Type of contract (official, TA or CA)	Function group, grade of recruitment*
Core Functions		
Level 1 Manager* (Executive Director & Deputy Executive Director) incl. Head of Directorate	TA	AD14 - AD 15
Level 2 Managers Head of Department* (eq. HoU)	TA	AD9 – AD11
Senior Specialist/Senior Analyst* (eq Senior officer)	TA	AD7
Specialist/Analyst* (eq Officer)	TA	AD6
Support Functions		
Head of Administration* (level 2 above)*	TA	AD11
Head of Finance (level 2 above)	No post at Europol	Notional AD9
Head of HR (level 2 above)	TA	AD9
Head of Communications (level 2 above)*	TA	AD9
Head of IT (level 2 above)	TA	AD11
Senior Specialist*	TA	AD7
Specialist* (incl. web editor)	TA	AD6, AST4
Admin Assistant or equivalent	TA/CA	AST2 / FGII
Special functions		
DPO*	TA	AD9
Accounting officer*	TA	AD9
Internal Auditor*	TA	AD9
Management Board Sec.*	TA	AD9

Please note function group and grade represents likely grade at appointment. With the transition Europol has staff occupying higher graded posts. Functions identified within Europol as close as possible given that there is no adequate definition of functions provided with the MSPP or following guidelines. Junior officer, senior/junior assistant, secretary, mail clerk, secretary to the Executive Director are not a recognised position at Europol. There is no equivalent.

---

[29] Laid down by Council Regulation (EEC, EURATOM, ECSC) No 259/68 and last amended by Regulation (EU, Euratom) No 1023/2013 of the European Parliament and the Council of 22 October 2013 (OJ L 287, 29.10.2013, p. 15)

Europol is responsible for its own recruitments and generally launches recruitment procedures through the announcement of vacant posts on its official website, and through the Europol National Units, in the social media and any other media as deemed appropriate. The vacancy notice provides information on the purpose of the post, tasks and responsibilities pertaining to the position, eligibility and selection criteria as well as terms and conditions of employment and outlines further details on the selection process. Employment at Europol is open to nationals of any of the 28 EU Member States. There is no nationality quota system in operation but Europol strives for a broad range of nationalities in order to keep a well-balanced geographical distribution among its staff members.

Candidates are recruited on the condition they are citizens of the Member States of the EU and are entitled to full rights as citizens. They also must have fulfilled any obligations imposed on them by the laws concerning military service and meet the physical and character requirements for the duties involved.

Owing to the nature of the Organisation activities, Europol, in cooperation with the relevant national authorities, shall initiate the security clearance process at national level immediately after the successful selection. In the meantime all candidates must present a certificate of good conduct.

All candidates are required to demonstrate knowledge of English, which is Europol's main language of internal communication. The required level of English knowledge is assessed during the written test and/or practical test and at the interview, in accordance with the requirements of the vacancy notice and the level of command that is necessary to perform the duties of the post. In addition, all candidates must fulfil the language eligibility requirement and provide evidence of a satisfactory knowledge of another language of the European Union (corresponding at least to B1 level of the Common European framework of reference for the levels of languages). This requirement will be checked by the Selection Committee based on the certificates and diplomas obtained by the candidate and, where necessary, further assessed during the selection procedure.

Europol has implemented a declaration of conflict of interest for the selected applicants. Before the employment contract will be concluded by Europol, successful candidates have to declare any conflict of interest situation.

Temporary Agents:

Temporary Agent posts are classified in two function groups according to the nature of the duties to which they relate: Administrators (AD) and Assistants (AST) in ascending rank order. Function group AD comprises twelve grades from AD 5 to AD 16. Based on the requirements of the Europol Regulation the posts within function group AD are divided further into two categories: posts that can be filled only by staff engaged from the competent authorities, called "restricted posts"[30] and "non-restricted posts" that can be filled by citizens of one of the Member States of the European Union who enjoy full rights as a citizen. Function group AST comprises eleven grades from AST 1 to AST 11. For AD posts AD6 is applied as entry grade in order to ensure it remains attractive for applicants who already have a career at national level. Furthermore it must be noted that limited real career perspective is possible at Europol, because maximum contract duration of nine years applies to the vast majority of staff. Europol seeks to use what flexibility it can when looking to recruit suitably qualified staff to fill its positions in order to fulfil its mission and reach its objectives.

---

[30] Decision of the Management Board of Europol defining the Europol posts that can be filled only by staff engaged from the competent authorities of the Member States EDOC~887871v25

Function	Summary duties and tasks
AD Function group:	
Executive Director	• Manages an administrative and operational entity of the highest level (Europol) in accordance with the Europol Regulation setting up Europol • Reports directly to the Management Board of Europol; • Provides leadership and direction to the organisation and assumes responsibility for performance of operations and strategic development; • Is Europol's legal representative; • Is Europol's delegated Appointing Authority; • Is Europol's Authorising Officer.
Deputy Executive Director (Head of Directorate)	• Assists the Executive Director in managing Europol by providing leadership and supervision to his Directorate and its relevant Departments; • Sets up, develops and monitors relevant strategies for his Directorate; • Replaces and represents the Executive Director as and when required.
Head of Department	• Provides leadership and direction in the Department, including the setting, implementation and delivery of policies and objectives; • Plans, directs and coordinates the use of the Organisation's resources in the delivery of the Department activities, maximising effectiveness and increasing efficiency; • Business planning, business evaluation and performance management within the Department, including responsibility for the quality of the Department's products and services; • Represents the Department and Europol (as appropriate) in internal and external meetings and conferences.
Head of Unit	• Supports the Head of Department with the day-to-day management and administration of the Department; • Leads the delivery of one or more of the products and services within the Department, as agreed with the Head of Directorate and Head of Department; • Ensures the quality and timeliness of the products and services delivered; • Manages and supervises staff in relation to those products and services; • Represents the Department in external and cross-departmental engagements.
Senior Specialist	• Engaged in providing expert knowledge and particular skills required at a highly developed level either in relation to a particular crime field or area of competence; • May include project management responsibilities and supervisory duties.
Senior Analyst	• Engaged in providing expert analyst knowledge and particular skills required at a highly developed level either in relation to a particular crime field or area of competence; • May include project management responsibilities and supervisory duties.
Specialist	• Engaged in providing specialist knowledge in relation to a particular crime field or area of competence; • May include advisory or supervisory duties.
Analyst	• Engaged in providing analytical knowledge of a particular work area or crime field.
Assistant Analyst	• Carries out data input, processing and administration in support of the analytical function and performs simple analysis under instruction in a particular crime field.

Function	Summary duties and tasks
AST Function group:	
Senior Officer	• Engaged in providing expertise and particular skills required at a highly developed level either in relation to a particular area of competence; • May include project management responsibilities.
Officer	• Provides specialist knowledge in relation to a particular area of competence.

Europol's selection procedures for Temporary Agents are governed by and conducted in line with the general implementing provisions on the use and engagement of Temporary Agents adopted in 2010.

Contract Agents

Contract Agent posts are classified in the four available function groups FG I to FG IV according to the nature of the duties to which they relate and the experience required.

Europol's selection procedures for Contracts Agents are governed by and conducted in line with the general implementing provisions on the use and engagement of Contract Agents adopted in 2010. The Commission decision of 16 December 2013 amending the Commission implementing rules on this matter is applied by analogy, insofar as it must be regarded as amending the implementing rules applicable at Europol.

Europol recruitment procedure for Temporary and Contract Agents

Equal Opportunity:
Europol applies a policy of equal opportunity for men and women and welcomes applications without distinction on grounds of sex, race, colour, ethnic or social origin, genetic characteristics, and language, religious, political or other convictions or opinions, financial situation, disability, age, sexual orientation, marital status or family situation.

Application process:
Candidates are required to complete the Europol application form in English. Candidates must specify whether a particular degree or course was full-time or part-time, the subjects covered and the official length of the course. Only diplomas issued by EU Member State authorities and diplomas recognised as equivalent by the relevant EU Member State bodies are accepted. If the main studies took place outside the European Union, the candidate's qualification must have been recognised by a body delegated officially for the purpose by one of the European Union Member States (such as a national Ministry of Education) and a document attesting so must also be submitted to enable the Selection Committee to accurately assess the level of qualification.
For "restricted" posts applications must be sent to Europol by the date of the deadline indicated on the vacancy notice at the latest. The stamp on the envelop serves as proof of the sending date. To apply for "non-restricted" posts the e-recruitment module available on Europol's website has to be used. Applications can, in this latter case, only be submitted until the day of the deadline. Applications received after the deadline cannot be accepted. Candidates who do not provide all necessary information, or apply after the specified deadline, or do not comply with any of the above will not be considered.

The Recruitment & Selection Team acknowledges receipt of all applications. Applicants invited to a written test/ practical test and interview will be required to send electronically in advance and provide, on the day of the written test, the following documents in original plus one copy:

- A document proving nationality (e.g. passport);
- Certificates attesting educational and professional qualifications with the information on the duration of that education mentioned in the application form;
- Documentary evidence of professional experience acquired after the date on which the qualification giving access to the specific profile was obtained, clearly indicating the start and end dates, whether paid, full or part time, and the nature of the duties carried out. Moreover, applicants must always provide a copy of the latest payslip as evidence of an ongoing employment contract.
- Written statement confirming that applicants for a restricted temporary agent posts are employed by one of the Member States' competent authorities, the application was submitted via National Unit and signed by the relevant Head of Europol National Unit (HENU).

Selection:

A Selection Committee is set up for each selection procedure on the basis of the ECSR and CEOS as well as applicable implementing provisions. The Selection Committee determines applicants' suitability for the position by assessing their qualifications, experience and skills and makes an initial selection from the applications received.

The responsibility for any decision made during this exercise lies with the Selection Committee. Failure to comply with one of the formal requirements or eligibility criteria will result in disqualification of the applicant(s) concerned.

Shortlisted applicants are invited to participate in a post-related selection procedure, generally consisting of written and/or practical tests and competency-based interviews / Assessment centre for the managerial posts/ designed to evaluate the capacities of the candidates to perform the key tasks outlined in the vacancy notice. During the interview special attention is paid to the specific knowledge for the post and the suitability and capacity of the candidates to adapt to a multicultural environment.

The work of the Selection Committee ends with the drawing up of a list of successful candidates which is submitted to the Executive Director. The Executive Director makes a decision on the most suitable candidate on the basis of the advice from the Selection Committee and informs the members of the Committee of her decision. All candidates who attend the selection procedure are informed of the outcome.

The Selection Committee's work and deliberations are confidential. It is forbidden for candidates to make direct or indirect contact with the members of the Selection Committee or for anyone to do so on their behalf. All enquiries or requests for information or documentation in relation to the competition should be addressed to the Europol Recruitment & Selection Team.

Data Protection:

Regulation 45/2001 applies to the processing of personal data carried out in the process of selection and recruitment of staff at Europol following the application of this Regulation to all administrative personal data held by Europol in accordance with Article 46 of the Europol Regulation.

Data controller

The controller of the processing operation upon your personal data is the Head of the Human Resources Unit.

Purpose of the collection of data

The data submitted is processed in order to assess the suitability of candidates for a position at Europol as temporary agent (TA), contract agent (CA), intern or trainee and to administrate the documentation related to the selection. The data collected in order to comply with this purpose are the ones required in the application form plus all data provided by the data subject in paper or electronic format. The purpose of the verification performed by Europol National Units on the candidates who apply online to the Restricted Annex II

posts is to ensure the conformity of the application process for members of a Competent Authority to a Restricted-Annex II post with the Europol Implementing Rules in force (Decision of the Management Board of Europol of 30 July 2010 laying down general implementing provisions on the procedures governing the engagement and the use of temporary agents at Europol).

Legal bases for processing personal data

The legal bases for the processing of personal data for temporary and contract agents are:
- Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities (Title III Chapter 1) and their implementing rules;
- Management Board Decision laying down general implementing provisions on the procedures governing the engagement and the use of temporary agents at Europol of 30 July 2010;
- Management Board Decision laying down general implementing provisions on the procedures governing the engagement and the use of contract agents at Europol of 13 October 2010.
- Decision of the Management Board of Europol defining the Europol posts that can be filled only by staff engaged from the competent authorities of the Member States ("restricted posts") of 13 December 2017.

The legal basis for the processing of personal data for interns is the Decision of the Europol Director on Internships of 15 March 2018.

Recipients of the data

Recipients of the data for the positions of temporary and contract agents are Europol staff employed in the Administration Department dealing with HR and financial matters, the members of the Selection Committee, the concerned Europol National Units (for restricted posts and restricted – Annex II posts), the Deputy Executive Director Capabilities and the Executive Director.

Recipients of the data for interns are Europol staff employed in the Administration Department dealing with HR and financial matters, the Supervisor of the intern and its superior line management as well as respective colleagues involved in the selection process and the Deputy Executive Director Capabilities.

Data storage and retention

All documents provided to Europol will be kept in Europol's files and will not be returned to the candidate. Applications of non-shortlisted candidates will be kept for a maximum of four years for temporary and contract agents. Data of non-recruited applicants on the reserve list for appointment will be kept for a maximum of five years after the expiry of the reserve list. Data of recruited candidates will be transferred to their personal file. Data of the selected interns will be kept for seven years after the finalisation of the selection procedure. The lists of the personal information (name, citizenship, date/ place of birth, address, telephone number) of the candidates who applied online for the restricted-Annex II posts sent to the concerned Europol National Units, to certify the validity of the status declared in the applications: civilian or member of a Competent Authority will be retained for verification by the respective Europol National Units for maximum 3 weeks after the closing date of the Vacancy Notice; they will be deleted after this period.

Rights as data subject

Candidates have the right to access, rectify, block and erase their personal data in accordance with the applicable data protection rules.

Contact in case of queries concerning the processing of personal data

Candidates have a right of recourse to the Europol Data Protection Officer (Europol - Data Protection Officer - Eisenhowerlaan 73, 2517 KK The Hague, The Netherlands) and the European Data Protection Supervisor (edps@edps.europa.eu).

Reserve list:

All candidates who attend a selection procedure are informed by letter whether they have been placed on a reserve list.

The reserve list is composed of candidates to be appointed to suitable posts should vacancies arise. Reserve lists are valid for a limited period of time (1 year), but can be extended for another year. Inclusion on a reserve list does not guarantee appointment. The information on the reserve list is available on the Europol website.

Contract Duration:
Temporary Agents will be offered an initial contract of up to 5 years renewable once for a maximum period of service of 9 years. Indefinite contracts may only be offered by Europol to staff occupying long-term posts (non-restricted) with the consent of the MB.

Contract Agents shall be engaged first for between 11 months and 5 years renewable once for a maximum period of services of 9 years. After successfully completing two fixed term contracts, an indefinite contract may be offered in line with the relevant implementing rules and decisions of the Executive Director and guidelines provided by the Management Board, where applicable. It should also be noted that in principal indefinite contracts may be offered at the outset.

European Communities Personnel Selection Office (EPSO):
Europol considers it important to preserve the opportunity to recruit staff that can provide knowledge as well as professional experience, given the need to ensure expert advice and operational support to the national competent authorities. Europol believes that the recruitment policies applicable to administrative services may not in all cases serve the interests of the Organisation and its customers; therefore, Europol follows a broader recruitment philosophy to ensure access to a specialised professional market, where necessary.

However, Europol recognises the important role that is played by EPSO in relation to maintaining standards, ensuring consistency and possibly providing candidates for Europol posts. It would be the intention to consider the use of EPSO where value might be added to the selection processes run in-house and subject to the availability of the required specialist knowledge within EPSO. Europol has a service level agreement with EPSO that allows Europol to place vacancies on EPSO's website.

Seconded National Experts

Seconded National Experts (SNEs) enable Europol to benefit from their high level of professional knowledge and experience and it is desirable to foster this exchange of professional experience by temporarily seconding experts from Member States to Europol. Any secondment must be authorised in line with Europol's annual budget. Profiles of SNE's sought are laid down in notices of secondment describing tasks and responsibilities as well as experience and skills required.

Eligibility criteria:
As described in Article 9 of the MB Decision laying down the rules on the secondment of national experts to Europol a SNE must possess at least 3 years of professional experience in the field of law enforcement relevant to the duties to be carried out during the secondment and produce evidence of a thorough knowledge of one Community language and a satisfactory knowledge of a second language.

Application process:
Secondment notices are forwarded to the Europol National Units via their Liaison Bureaux and are published on IRIS and Europol website as well for a minimum duration of 28 days. Candidates endorsed by the national competent authorities are required to complete the application form and submit the original application via their National Unit to Europol. The application form must be accompanied by a letter from the sending authority to the Executive Director of Europol expressing willingness to second the candidate. Applications must be sent to Europol by the date of the deadline indicated on the vacancy notice at the

latest. The stamp on the envelop serves as proof of the sending date. Applications received after the deadline cannot be accepted.

Selection:

A Selection Committee chaired by the Head of the relevant Directorate or a senior representative and composed by a representative of the respective Unit as well as the HR Unit determines the suitability of candidates by assessing their skills, experience and qualifications in relation to the notice of secondment and makes an initial selection from the applications received. For the initial selection, the operational contributions from the competent service to the project to which the SNE will be seconded are taken into account. The Selection Committee conducts a telephone/Skype interview with the shortlisted candidates in order to evaluate their language skills, to validate their experience and to assess whether they possess the key skills required.

Depending on the profile of the secondment, the tasks and responsibilities pertaining to the position and the skills required, shortlisted candidates might be invited to attend a selection procedure at Europol, consisting of a test or comparable practical exercise and an interview. In the basis of the outcome of the telephone interview or the selection procedure the Selection Committee makes a recommendation for the Deputy Executive Director Capabilities (DEDC) to endorse.

The secondment is finally authorised by the DEDC and effected by an exchange of letters between the DEDC and the seconding authority, specifying the details of the secondment as described in the MB Decision.

Duration:

Periods of secondment, including any extension, shall not exceed a total of 4 years.

Cost-free Seconded National Experts

Europol can exceptionally engage cost-free SNEs in the following cases:

Upon request of Europol

In case a new operational need arises after the elaboration of the work programme and budgetary resources are not available for additional SNEs, Europol can engage SNEs on a cost-free basis and will specify in the notice of secondment that Europol does not cover any expenses other than those related to the performance of duties during the secondment. This provision is intended for highly exceptional situations.

Upon request of a Competent Authority

If a Competent Authority expresses an interest to start a new project or to extend the scope of an existing project with new products or services a business case outlining how the seconded expert will contribute to the work programme of the Department and what additional products, services or improvements will be introduced must be compiled by the Competent Authority. This business case has to be sent via the Europol National Unit to Europol's HR Unit, together with an accompanying letter addressed to the Executive Director formally supporting the secondment as well as an application form completed by the seconded expert. Upon receipt Europol will assess the feasibility of the secondment and will make a recommendation to Directorate Management and the Executive Director.

In case a seconded expert is engaged cost-free Europol can waive the requirement to interview the candidate.

Structural service providers[31]

The use of structured service providers (contractors) occurs across Europol in various work areas. A number of service providers are engaged in providing reception duties for the HQ and basic clerical activities and for specific security services supporting the security services provided by contract agents. The security staff and reception services are engaged through dedicated open tender procedures.

---

[31] NB Structural service providers are not employed by the agency.

The majority of these staff is, however, engaged within the ICT functions at Europol where they provide helpdesk support, software development and technical assistance. The utilization of structured service providers in ICT is envisaged to stabilise over the planning period. External service providers will be used as staff augmentation to cope with increasing volumes and additional tasks. Services are provided in the following areas:

- ICT Development services
- Project Management Services
- Testing services
- Project Support services
- Help desk services
- Infrastructure/operations expert services
- ICT Standards and procedure services

During the year certain other staff may be engaged in Turnkey projects; in this case these staff work on the delivery of projects but are not separately identified in the MSPP.
All contractors are engaged after the conclusion of the appropriate tenders, which are run in accordance with the financial regulation and appropriate guidelines.

For those staff engaged to fulfil ICT related tasks, framework contracts have been established with a number of individual companies associated with the contract. When a new need is identified a new process is opened whereby interested companies submit new offers for the services that are considered by Europol and awarded in line with the necessary provisions.

Most contractors are engaged through group contracts or framework contracts. The duration of their service at Europol varies from a number of months to a number of years, depending upon the nature of the contract.

Annex IV:

B. Appraisal of performance and reclassification/promotions

Appraisal

Europol's first implementing rule on appraisal was adopted in October 2011. The first exercise was run in January 2012 to cover the period from the change to agency status until 31/12/2011. The appraisal exercise has been repeated every year.

The appraisal process was reviewed in 2014 to comply with the new EU Staff Regulations. The Management Board approved on 15.09.2014 for temporary agents the application by analogy of the Commission Decision C(2013)8985 of 16.12.2013 laying down general provisions for implementing Article 43 of the Staff Regulations and implementing the first paragraph of Article 44 of the Staff Regulations. Similarly for contract agents the Commission Decision C(2014)2226 on general provisions for implementing Article 87(1) of the Conditions of Employment of Other Servants of the European Union and Implementing the first paragraph of Article 44 of the Staff Regulations Commission Decision was approved on 03/12/2014.

Reclassification

Reclassification was for the first time implemented at Europol in 2014. The Management Board adopted the (unchanged) Commission Decision C(2013)8968 of 16 December 2013 laying down general provisions for implementing Article 45 of the Staff Regulations. These general provisions applied to the reclassification organised in 2017 for the temporary staff and contract staff.

Reclassification of temporary staff

Category and grade	Staff in activity at 01.01.2016		How many staff members were promoted / reclassified in 2017		Average number of years in grade of reclassified/ promoted staff members
	officials	TA	officials		
AD 16		0		0	
AD 15		1		0	
AD 14		1		0	
AD 13		2		0	
AD 12		6		0	
AD 11		12		1	7.58
AD 10		9		1	6.92
AD 9		47		3	5.14
AD 8		81		1	3.42
AD 7		91		5	3.26
AD 6		134		9	3.44
AD 5		9		3	3.05
Total AD		**393**		**23**	
AST 11		0		0	
AST 10		0		0	
AST 9		0		0	
AST 8		0		0	
AST 7		3		0	
AST 6		4		0	
AST 5		6		0	
AST 4		9		1	7.17
AST 3		3		0	

Category and grade	Staff in activity at 01.01.2016		How many staff members were promoted / reclassified in 2017		Average number of years in grade of reclassified/ promoted staff members
	officials	TA	officials		
AST 2		2		0	
AST 1		0		0	
Total AST		**27**		**1**	
Total		**420**		**24**	

Reclassification of contract staff

Function Group	Grade	Staff in activity at 01.01.2016	How many staff members were reclassified in 2017	Average number of years in grade of reclassified staff members
CA IV	18	0		
	17	0		
	16	1		
	15	3		
	14	14	2	4.98
	13	8	2	3.44
CA III	12	0	0	0
	11	13	2	4.00
	10	34	7	7.01
	9	22	1	3.00
	8	8	4	3.03
CA II	7	0	0	
	6	4	1	3.50
	5	26	2	2.44
	4	1	0	
CA I	3	0	0	
	2	0	0	
	1	0	0	
Total		**134**	**21**	

Annex IV:

C. Mobility policy

a) Internal mobility

Europol has an internal mobility policy promoting the development of a register where staff can express interest in moving within the organisation. Applications are assessed on the basis of business need. A register has been set up as a way of gathering information about staff interested in internal mobility, without prejudice to the applicable rules and regulations which are observed for all reassignments, whether at the initiative of the staff member or the agency. A coherent, transparent and fair internal mobility policy is an incentive for staff to remain and stay motivated. The current policy is currently under review in light of new Implementing Rules.

b) Mobility between agencies and Institutions

Once the model decision on the general implementing provisions on the procedure governing the engagement and use of temporary staff under Article 2(f) of the CEOS has been approved by the Management Board it will be implemented at Europol.

The following tables provide for 2017 the numbers of staff that were recruited from other EU institutions and agencies and the numbers of staff that were recruited by other EU Institutions and agencies:

Europol Staff in post as per December 2017 recruited from:	Number
European Institutions	
European Commission	4
EU Agencies	
Eurojust	1
FRONTEX	1
ESMA	1
CEPOL	1
Other	
Total	**8**

Europol Staff leaving post during 2017 recruited by:	Number
European Institutions	
European Parliament	1
European Commission	2
OLAF	2
EU Agencies	
EIB	4
EASO	1
EFCA	1
Eurojust	2
Frontex	5
Total	**18**

Annex IV:

D. Gender and geographical balance

Gender balance

In a more equal organisation, in which individuals' different knowledge and experience are utilised, the activities and results improve along with the development of new ideas and the stimulation of new thinking. Europol applies a policy of equal treatment for men and women and welcomes applications without distinction on grounds of sex, race, colour, ethnic or social origin, genetic characteristics, and language, religious, political or other convictions or opinions, financial situation, disability, age, sexual orientation, marital status or family situation.

One of the main sectors for Europol's recruitment is law enforcement organisations, which could entail limitations in relation to gender balance. Europol will increase its efforts in partnership with the Member States' Competent Authorities to improve the gender balance.

Gender breakdown at Europol (on 31.12.2017)

Post	Gender	Number	Percentage
Temporary Agents	Female	149	28%
	Male	386	72%
AD Function group	Female	127	25%
	Male	379	75%
AST Function group	Female	22	76%
	Male	7	24%
Contract Agents	Female	88	55%
	Male	72	45%
Seconded National Experts	Female	24	22%
	Male	85	78%
Overall	Female	261	32%
	Male	543	68%

Europol remains concerned about the gender representation in the organisation. Europol continues to work on the issue and continues to maintain feasible targets for the recruitment of women to AD posts and the appointment of women to senior specialists and middle management posts. The long-term target is that gender balance will be closer to 60/40% in each staff category and in Europol as a whole.

In general, this involves inter alia to:

- address barriers to career development of women;
- reconcile personal and professional life;
- improve the gender balance;
- make a comparative study of careers;
- sensitize staff to gender equality and equal opportunities;
- protect the dignity of the person in the workplace.

Europol strives to:

- encourage a better participation of women in external competition boards, in internal selection processes and by encouraging female Temporary Agents to participate in Europol's management training;
- identify the factors which influence the career development of men and women in the AD Function Group;
- develop a gender-sensitive work culture which takes account of female and male values, of differences in attitudes, in priorities, in working methods, as well as of gender specific needs;
- make adjustments in the organisation of work to improve the compatibility with family responsibilities, and in the operation of personnel policies;
- enhance an even share of responsibilities and increased involvement of women in decision-making, as well as their professional development throughout their career;
- modernise recruitment and career policies, as well as certain social infrastructures;
- establish accompanying measures for the reconciliation of professional and private obligations.

Specific strategies:

- Removing barriers to the career development of women and improving the gender balance.
- Actions in relation to recruitment and selection;
  - Selection of an underrepresented sex when merits are equal
  - Gender balance in the composition of selection panels where possible
- Advertisement of vacancies in a gender neutral manner;
- Actions in relation to training;
- Actions in relation to career development;
- Equal treatment regarding promotions;
- Measures concerning mobility and career guidance.

Europol, like other agencies, continues to promote the use of policies and procedures to encourage family friendly working conditions within the framework of the EUSR. A positive approach is taken with the implementation of the new working time regime allowing for flexible working arrangements and the possibilities for part-time work and parental leave.

A "gender balance" project ran from 2012 to 2014 and the findings of this initiative are reflected in the measures described above.

Geographical balance

The table below provides an overview of staff from each EU Member State working at Europol as on 31.12.2017.

Country	TA's			CA's	SNE's	Total	Europol Liaison Officers, whilst working at Europol do not form part of the staff of the organisation and are thus excluded from the total figures but included for information only	ELO's
	AD	**AST**	**TOTAL**					
Austria	7	0	7	1	1	9		8
Belgium	31	1	32	1	2	35		2
Bulgaria	14	2	16	8	3	27		2
Croatia	10	0	10	1	7	18		1
Cyprus	2	0	2	0	1	3		2
Czech Republic	12	1	13	1	1	15		3
Denmark	1	0	1	0	4	5		4
Estonia	6	0	6	0	0	6		4
Finland	11	1	12	3	1	16		4
France	35	1	36	7	8	51		12
Germany	38	2	40	5	8	53		11
Greece	39	1	40	12	4	56		1
Hungary	12	1	13	9	3	25		5
Ireland	9	0	9	0	0	9		4
Italy	30	2	32	13	22	67		7
Latvia	3	1	4	1	0	5		2
Lithuania	5	1	6	2	1	9		4
Luxembourg	0	1	1	0	0	1		4
Malta	2	0	2	0	0	2		1
Netherlands	44	7	51	48	1	100		26
Poland	29	3	32	5	3	40		5
Portugal	21	0	21	5	2	28		1
Romania	48	0	48	10	4	62		2
Slovakia	6	0	6	0	1	7		3
Slovenia	8	1	9	3	0	12		2
Spain	50	2	52	18	27	97		11
Sweden	5	0	5	2	0	7		8
United Kingdom	28	1	29	5	5	39		20
Third States/ Organisations	0	0	0	0	0	0		61
Total EU MS	**506**	**29**	**535**	**160**	**109**	**804**		**159**
Overall Total	**506**	**29**	**535**	**160**	**109**	**804**		**220**

Annex IV:

E. Schooling

The European School adds to the education facilities currently provided in The Hague. Children of expatriate staff currently attend the International School, the British School Netherlands, the French Lyceum, the German International School, the American School or the Lighthouse. Alternatively they may attend Dutch schools, based on parental choice.

The establishment of the European School of The Hague was agreed in 2011 and it opened its doors in school year 2012/2013. The school is based in the International Zone within The Hague and is an accredited European School which, although not forming part of the network of European Schools organised by the intergovernmental organisation 'The European Schools', offers a European education that meets all pedagogical requirements laid down for European Schools. It is set within the framework of the Dutch national school network and thus remains outside the legal, administrative and financial framework to which the European Schools are compulsorily subject.

For its accreditation, the school is regularly visited by the European accreditation inspectors who provide a separate recommendation on the Primary and Secondary departments. In addition, the school regularly received the Dutch school inspectors.

When the school opened it started with three language sections: English, Dutch and Spanish. Since then, there have been developments in the offerings of language sections. In September 2014 the school opened a German and a French Nursery class as well as a French Primary 1 & 2 class. A Spanish language section is not foreseen in the secondary school programme and secondary classes were opened in the English, Dutch and French section. The children currently in the primary classes of the Spanish section will integrate into these language sections.

In school year 2012/2013 the school offered education to children in Nursery years 1 and 2 and Primary years 1 and 2. This was followed by Primary years 3, 4 and 5 in 2013/2014, since then offering the full Primary school programme. The Secondary school programme commenced with years 1 – 3 in 2014/2015, gradually opening additional classes in each section. Since the start of 2017/2018 the Secondary school offers Year 5 in English, Dutch and French and Year 6 in English. According to the envisaged schedule one extra level will be opened per school year; however, the precise schedule for opening secondary years 6 – 7 in the different language sections can, at this moment, not yet be confirmed as the opening of a year in a language section depends on the number of enrolments for that particular year. It is expected that the first European Baccalaureate will be awarded in school year 2018/2019.

For school year 2017-2018, 1095 pupils have been registered in the school, of which 769 children attend Primary education and 326 children attend Secondary education. More than a quarter of this total, i.e. 291 pupils, are children of Europol staff (212 in Nursery & Primary and 79 in Secondary). In addition, 41 children of SNE's and Liaison Officers have enrolled, therefore Europol's workforce accounts for almost one-third of the pupils enrolled in the European School The Hague.

Due to the growth of the school the Executive Director of the Stichting Rijnlands Foundation and the school management of the European School have decided, with support of the municipality of The Hague, on the opening of a second location as the school's initial expansion plans of the current facility were not sufficient to cope with the demand. In March 2017 the school location Oostduinlaan 50, the historical school building of the former Aloysius College, was officially appointed to the European School The Hague. The school building needs thorough renovation to make it suitable for the pupils. It is foreseen that the secondary department of the ESH will move into the second location as per fall 2018. Initially the pupils will be housed in temporary classrooms until the renovation has been completed.

The Advisory Board of the school, which consists of representatives of the four European Agencies in The Hague vicinity (Europol, Eurojust, ESA/ESTEC and EPO) is involved in the developments and provides strategic advice for the further development of the school.

Annex V: Buildings

	Name, location and type of building	Other Comment
Information to be provided per building:	Headquarters, Eisenhowerlaan 73, 2517 KK, The Hague Netherlands	The Dutch Government Buildings Agency is owner of the building. Europol is responsible for the user related elements which are linked to the business of the organisation e.g. catering, ICT, Security and AV systems.
Surface area (in square metres)	Gross floor space building is 32.500 m^2.	Number of workplaces has increased from 850 to 1,132.
Annual rent (in EUR)	N/A	Building provided free of charge by the Host State.
Type and duration of rental contract	Lease Agreement is valid for 20 years and was signed on 1 March 2011.	Lease Agreement Europol New Headquarters, reference EDOC-#532152.
Host country grant or support	Host State support by providing and maintaining the accommodation.	The maintenance regarding the owner related elements.
Present value of the building	N/A	

Building projects in planning phase:
In 2016 Europol started a multi-year project (2017-2019) together with the Host State to replace the Audio-Video (AV) installations of the conference environment and the cabling from analogue to digital. The AV alterations are based on technical life-cycle and new technologies which are needed to assure the business continuity and be in compliance with the actual quality (ICT, interpretation and conference) standards. The AV installations are defined in the Lease Agreement as user elements which means that they have to be paid by Europol. Following the design and tendering phases in 2016 and 2017, implementation started in March 2018 and is scheduled to be completed Q1/2019.

Europol is facing a shortage of workplaces and meeting facilities in its headquarters. The Dutch Host State and Europol have developed a Strategic Housing Roadmap (SHR) for the period 2016 – 2031 (expiration of the first term Lease Agreement). For the mid-term, the capacity of the building should increase from 1,132 to approximately 1,200 workplaces by creating extra workplaces via a new office concept, which includes implementing a workplace ratio of 0.84 per workplace to accommodate 1,400 people in the building and to increase the meeting facilities. The necessary construction works had to be delayed due to the floor slabs issue[32] and are now planned to start in 2020.

Additionally, a total of 190 staff will be relocated to a temporary satellite building as a Mid-Term Housing Solution in order to cover Europol's growth and to allow for the implementation of the new office concept at the HQ. The satellite building needs renovation and its delivery is planned for Q3 2019.

Based on the growth prognosis it can be expected that the maximum capacity of the HQ will be reached in 6 years. A working group with the Host State is established to investigate the housing potentials in the surrounding of the HQ for a permanent expansion which should be available by the end of 2023. A strategic vision for the Long Term Housing Measures will be finalised by 2018 and will be used as basis for drafting the functional and technical requirements of the new building. Construction of the new permanent facility is expected to start in 2021 and be finalised by the end of 2023.

---

[32] Following a serious incident at a parking building at Eindhoven airport caused by issues related to prebuilt concrete floor slabs, the Dutch Host State implemented a national procedure to check all public buildings where these specific floor slabs have been used, including Europol's HQ. Research on the issue is still ongoing and should be concluded by Q2 2019.

Annex VI: **Privileges and immunities**

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	**Education / day care**
According to Article 63(1) Europol Regulation the Protocol on Privileges and Immunities of the European Union ("Protocol No. 7"[33] to the Treaty on European Union and the Treaty on the Functioning of the European Union) applies to Europol.

The Protocol is supplemented by the Agreement of 15 October 1998 between the Kingdom of the Netherlands and Europol concerning the Headquarters of Europol (*see Art. 70 Europol Regulation*). | According to Article 63(1) Europol Regulation the following legal acts apply to Europol's staff (including the Executive Director and the Deputy Executive Directors):

- Protocol on Privileges and Immunities of the European Union ("Protocol No. 7" to the Treaty on European Union and the Treaty on the Functioning of the EU)

- Regulation (Euratom, ECSC, EEC) No. 549/69 of 25 March 1969 determining the categories of officials and other servants of the European Communities to whom the provisions of Article 12, the second paragraph of Article 13 and Article 14 of the Protocol on the Privileges and Immunities of the Communities apply (as last amended by Regulation (EC) No. 371/2009 of 27 November 2008)

Protocol and Regulation are supplemented by the Agreement of 15 October 1998 between the Kingdom of the Netherlands and Europol concerning the Headquarters of Europol (*see Art. 70 Europol Regulation*), which is itself supplemented regarding staff privileges and immunities by an exchange of *Notes Verbales* of 24 October 2007. | Europol staff members can benefit from the ordinary rules regarding tax benefits linked to day care expenses just as any other residents of the Netherlands. |

---

[33] Please note: Protocol No. 7 has been renumbered, compared to the Protocol on Privileges and Immunities of the European Communities. Its Article 15 empowers the European Parliament and the Council to determine acting by means of regulations the categories of officials and other servants of the Union to whom the provisions of Article 11, the second paragraph of Article 12, and Article 13 of this Protocol shall apply, in whole or in part. -Regulation No. 549/69 (see above) has not been amended following the entry into force of the new Protocol No. 7 (1 Dec. 2009), thus still contains the references to the old numbering.

Annex VII: Evaluations[34]

Internal monitoring & evaluation

Europol management monitors the implementation status of all planned actions, projects and indicators on a quarterly basis, to assess the overall progress and to take corrective actions where needed.

Under Europol's previous regulatory framework, the **Six-Month Activity Report** was prepared by Europol and presented to the Management Board in accordance with Article 38(4)(j) of the Europol Council Decision. This article stipulated that regular reports on the results of **monitoring Europol's performance in terms of achievement of its objectives** were to be submitted to the Management Board.

Under the Europol Regulation (ER), which became applicable in May 2017, there is no reference to a similar article. However, when the **Six-Month Report 2016** was presented to the MB, at the October 2016 meeting, it was unanimously agreed to continue with the production of this report under the new Europol Regulation.

The report covers the period from 1 January until 30 June and presents the progress made against the annual targets set for the Strategic Key Performance Indicators (KPI) and Work Programme objectives. It also includes an overview of main achievements. Finally, the report includes an overview of the budget implementation and human resources management, main identified risks, the efficiency and effectiveness of the internal control system and audit results.

Actions and projects are considered on track when their status is on-going as planned or already completed. Indicators are considered on track when their targets have been achieved. In addition, actions or projects that have been deprioritised / cancelled because of external or unplanned factors are considered as not on track, therefore negatively affecting the reported performance. This means, in practice, that Europol is applying strict standards when assessing the performance against its objectives.

The **Consolidated Annual Activity Report (CAAR)** is submitted on behalf of the authorising officer of Europol on the duties and activities performed on annual basis. It is presented in accordance with Article 47 of the Financial Regulation applicable to Europol, which stipulates that the authorising officer shall report to the management board on the performance of his/her duties in a form of a consolidated annual activity report.

The report covers the period from 1 January to 31 December and presents the progress made against the annual targets set for the KPIs linked to Europol's Strategy and the implementation of the annual Work Programme objectives. It is following the template provided by the Commission and developed by the EU Agencies Network – Performance Development Network (PDN) for the preparation of the Consolidated Annual Activity Report.

Furthermore, this document provides an overview of budget implementation, human resources, risk management activities, efficiency and effectiveness of the internal control system and audit results. An analysis and assessment of the CAAR is made by the Management Board. All building blocks of assurance are also included in the relevant parts of the report.

The **Internal Control Standards (ICS)** were adopted by the Management Board in 2011. The implementation of the ICS focuses on continuously refining organisational processes and identifying key internal controls which need further development/review in order to ensure proper process implementation and reduction of the risks related to process performance. In this context, it should be noted that in the course of 2017, the ICS have been replaced by an Internal Control Framework (ICF) of the European Commission which follows a comparable governance approach as before under the ICS. In light of the new ICF of the European Commission, the Management Board adopted the Europol **Internal Control Framework (ICF)**, as provided for in Article 44 (2) of the FR applicable to Europol, in

---

[34] Figures provided in Annex VII present the situation as of 30.06.2018.

December 2018. The ICF applies as of 2019, thereby replacing the ICS adopted by the Management Board in 2011.

In accordance with its Audit Plan and as reported in Europol's Sixth-Month Activity Report 2018, the **Internal Audit Capability (IAC)** completed, in the first semester of 2018, an assessment of the application of the Europol Regulation and a follow-up exercise on past recommendations issued by the IAC in the period 2010-2016. By the end of 2018, the IAC finalised an audit engagement on Europol's on-the spot operational support to Member States and one on learning, training and development of Europol staff, and on the validation of user access rights granted in ABAC. In its consultancy function, the IAC was requested and provided input and advice on the evolution of the MB Working Group on ICT into a Working Group on Information Management and on the cooperation with the ATLAS network. Europol provided a report on the overall status of implementation of recommendations issued by the IAC to the Management Board in 2018. Further granular reporting will be included in the Six-Month Activity Report and CAAR for 2019.

During the first six months of 2018, the **Data Protection Function (DPF)** continued working on reviewing the compliance of Europol's processing operations with the applicable legal regime. This included a compliance check in the area of "processing personal data originating from private parties" within the (old) Europol Analysis System. As a result of this check, three very important recommendations were issued.

In addition, the DPF regularly takes care of data subjects' requests (Art. 36 requests). Article 36 ER grants the right to any data subject, at reasonable intervals, to obtain information on whether personal data relating to him/her are processed by Europol. In the first six months of 2018, 209 requests were handled representing an increase of 31% compared to the same period in 2017. These requests resulted in four full hits and six partial hits with Europol's databases.

Furthermore, the Europol Regulation introduces in Article 39 a requirement for prior consultation. According to Article 39 ER new types of (operational) processing operations that include processing of sensitive categories of personal data and/or data that present a specific risk for the fundamental rights and freedoms of data subjects, and that have been launched or substantially changed after 1 May 2017, are subject to prior consultation with the European Data Protection Supervisor. In the context of Article 39, the DPF has established and documented the respective process in close consultation with all Europol Directorates. In 2018, prior consultations relating to the 'Querying Europol Systems (QUEST)' application, the European Tracking Solution (ETS) and for extending Member States' access to the "Internet Referral Management Application" (IRMA) were initiated.

In addition, the DPF had several meetings with ICT to further improve the way the audit log information was made available within the Unified Auditing System (UAS). The DPF also performed the business validation of the audit log information related to the new QUEST release. Moreover, the DPF created a number of scheduled reports, not containing any personal data, in order to automatically notify relevant stakeholders about data quality and data protection issues (e.g. person implication missing in the EAS). Regarding the further development of the IDMC, the DPF was involved in various discussions and projects, relevant to the subject, and participated in several meetings on the "Search and Cross-check" value-stream architecture, leading to the amendment of some process descriptions and the follow-up of hidden hits in the EIS.

External monitoring & evaluation

The IAS, supported by the IAC and Europol, performed a risk assessment on Europol's governance, administrative and support process areas in May 2017. This exercise is performed at Europol every four years, with a view to identifying the overall risk profile of key administrative processes outside the core business area. On the basis of the risk assessment concerning Europol's process landscape, the Europol MB endorsed the "IAS Strategic Audit Plan 2018 – 2020" in October 2017. The following audit topics were identified in the strategic audit planning, in the following order: (a) HR Management (including the sub-processes: performance appraisal/career development and planning), (b) IT security, (c) contract management (including the sub-processes: planning, monitoring of activities,

procurement and budget execution), (d) anti-fraud strategy and ethics (including the sub-processes: ethics/ethical behaviour, risk management and fraud prevention), as a reserve topic.

In 2018, the IAS performed an audit on HR Management (including Recruitment) and Ethics. Following a common approach on HR Management audits, the IAS included the ethics component in the initial audit scope. In order to assess the overall HR function in its complexity and given the importance of recruitment for the success of the organisation the scope of the audit work was further expanded to include the recruitment process. In addition, the IAS launched a survey among Europol staff to gather perceptions and feedback on HR management and ethics, the results of which will be addressed in the audit report that will be released at the beginning of 2019.

Regarding audit engagements performed by the IAS in the past, there are 2 pending recommendations, graded as important, stemming from the audit on stakeholder management conducted in Q1 2015. Europol considers all other five pending recommendations as implemented. A formal review of the status of the recommendations is expected to be performed by the IAS in due course.

The **European Data Protection Supervisor (EDPS)** was very active with the supervision of Europol's activities in the first semester of 2018. In the course of its supervisory activities, the EDPS established a dedicated team for Europol's Supervision and Enforcement composed of six permanent staff members dealing exclusively with Europol matters. Overall, the DPF established a professional and welcoming working relationship with the EDPS and the 2017 annual reports of both the EDPS and the Data Protection Officer of Europol illustrate an excellent record of cooperation. In 2018, the main areas of supervision focused on: (a) the Europol Analysis System and the related functionalities; (b) the embedment of FIU.net into SIENA with a view to data protection and information security related concerns; (c) On-going EDPS inquiries (Art 34(2) ER) on EAS compliance with the Europol Regulation; (d) the second EDEN Conference planned for the end of November at Europol.

The audit activities performed by the **European Court of Auditors (ECA)**, supported by an external audit contractor as described in Article 107 of the Financial Regulation applicable to Europol, concerning the annual accounts of Europol for 2017 and the related implementation of the Delegation Agreement and the Hotspot Grant Agreement were carried out between January 2018 and the end of 2018.

Europol received positive audit opinions on the implementation of the Delegation Agreement, the Hotspot Grant Agreement and the annual accounts.

On 22 June 2018, the Europol MB adopted the opinion on the final annual accounts which were submitted to the ECA, the European Commission's Accounting Officer, the discharge authority (Council and the European Parliament), and the national parliaments on 29 June 2018. The ECA's assurance statement to the discharge authority will comprise a positive opinion in relation to the reliability of the accounts, as well as the legality and regularity of the financial transactions underlying the 2017 annual accounts. The discharge proceedings concerning the 2017 financial year will be completed under the lead of the European Parliament in Q1 2019.

Annex VIII: Risks 2019

Europol's corporate risk management process aggregates risks (including the related responses) at organisational level. In doing so, Europol expands risk management from a vertical (e.g. in departments or programmes/projects) to a horizontal perspective (corporate, organisational wide view), meeting the required elements on risk management set out in the Internal Control Framework (ICF) of Europol[35], which is based on the COSO ICF[36] and the European Commission's ICF[37]. In line with this, corporate risks are considered internally by Europol at regular intervals throughout the year and on an immediate ad hoc basis in the event of the identification of time-critical or high impact risks.

For Europol, a risk is an uncertain event or set of events that, should it occur, would have an effect on the achievement of objectives related to the annual business planning (i.e. Work Programme and the related internal Work Plan). Risks are understood in two dimensions: **Threats** (expected negative effect on a business objective) or **opportunities** (expected positive effect on a business objective). Both types of risk – those identified as threats and opportunities – are listed below. The overview only shows critical risks.

A **critical risk** is defined as a potential event or set of events in the future where the **impact** of the risk concerned is assessed as **severe** (meaning the concerned objective could not be reached at all (threat) or easily be achieved (opportunity) in comparison with the given planning) and the **probability** is considered to be **high** (i.e. the risk event – threat or opportunity – is likely to occur).

Given the current risk exposure concerning the business planning, the following critical risks (threats) are identified for the 2019 planning[38]:

---

[35] Internal Control Framework (ICF) of Europol, Europol file no. EDOC #951032v13
[36] Committee of Sponsoring Organisations of the Treadway Commission (COSO) Internal Control Integrated Framework, May 2013
[37] Communication to the Commission – Revision of the Internal Control Framework, C(2017) 2373, Europol file no. EDOC #911042v1
[38] It should be noted that the critical risks, in terms of threats and opportunities, represent a "snapshot" moment in time. The risks described are integrated into the risk register as part of the corporate risk management process at the end of 2018 (for follow-on monitoring in 2019). This will ensure that the risks are regularly assessed and amended where required. The Europol MB is informed of any significant change to the risks presented on the following pages.

(1) Overview of threats (risks which could have a negative effect on the 2019 business planning)

Ref. nº	Risk description (cause, event and effect)	Objective area	Response type[39]	Key Response measures
01	Europol may not meet the operational demand identified in the Europol Strategy 2016-2020[40] and the strategic priorities 2020+ presented to the Management Board in December 2018, thus may not deliver a unique and valuable set of operational support services according to expectations of Member States, cooperation partners, including the needs of front-line investigators, as well as political expectations, due to the lack of: • Speed, relevance as well as quality of operational response and analysis provided; • Capabilities which allow for direct, secure and user-friendly communication, in real time, during operations; • First-hand and live access – at federal, regional and local levels – to serious organised crime and terrorism related investigative data during operations supported by Europol, in particular on-the-spot at the request of national authorities (as part of EMIST, EMAST, hotspot deployments and in the EU RTF); • Member States' preparedness to share live, high quality investigative data (including relevant context) with Europol, reflecting sufficient awareness of, or trust in, Europol's capabilities as an operational partner; • Progress on operational cooperation between the ECTC and Member States' CT competent authorities, including security services through the CTG members especially; • Adequate cyber investigation support to counter-terrorism, as well as EU IRU capabilities to effectively respond to radicalisation and terrorism propaganda online and an EU TFTS mechanism; • Europol's capability to effectively and efficiently process and analyse contributions, next to private matching capabilities; • Effective coordination of law enforcement activities against cross-border organised crime affecting the EU, based on an accurate and	A.1.1 A.2.1 A.2.2 A.2.3 A.3.1 A.3.2 A.3.3 A.3.4 A.3.5 A.3.6 A.4.1 A.4.3 A.5.1 A.5.2 A.6.1 A.6.2 A.6.3 A.6.4 A.7.1 A.7.2	Share	• Advance the implementation of the new information management architecture and continue improving operational capabilities and tools by focusing on automation and modernisation (Objective A.1.1); • Broaden the information processing capabilities of Europol's Front Office (Objective A.2.1); • Utilise the newly acquired access of Europol to the Schengen Information System (Objective A.2.2); • Implement an effective cooperation process with external partners on the basis of Europol's External Strategy 2017-2020 (Objective A.2.3); • Ensure the implementation of the objectives of the Malta Implementation Plan in the fight against organised crime related to migrant smuggling and THB (Objectives A.3.2); • Undertake and support further improvements in the strategic and operational approach followed by the Member States and Europol in targeting the reduction of drugs supply (Objective A.3.3); • Strengthen the fight against counterfeiting and intellectual property crime (Objective A.3.4), organised crime groups involved in fraud activities (objective A.3.5), organised property crime (A.3.6); • Improve procedures and operational approach to foster Europol's support to MS investigations against organised crime (A.3.1); • Accelerate Europol's capabilities to provide support to Member States' investigations in the area of cybercrime-related EU Policy Cycle priorities 2018-2021 (Objective A.4.1);

---

[39] Threat risk type responses are: Reduce (pro-active actions are undertaken to minimise the probability or impact; the responsibility for the risk effect(s) and response measure(s) stay with Europol); Remove (changing the scope of the business objective concerned); Transfer (a third party takes responsibility for the risk); Retain (conscious and deliberate decision to accept the risk and, especially, the possible effect(s) on the business objective); Share (the responsibility for the risk effect(s) and risk response measure(s) are shared between the involved parties, i.e. Europol and Member States take responsibility for certain aspects of the risk)

[40] "effective and immediate first-line information exchange", "enhance cooperation in the area of counter terrorism" and "high quality analytical support" to support serious organised crime, illegal migration, cybercrime and terrorism investigations

Ref. nº	Risk description (cause, event and effect)	Objective area	Response type[39]	Key Response measures
	thorough understanding of priority crime areas and emerging (regional) threats; • Enhanced operational cooperation with third parties and source countries for key crime areas and relevant countries/bodies on a global scale, given new cooperation agreement mechanisms under the Europol Regulation (including continued operational cooperation with EU Member State authorities that are not part of the Europol Regulation); • Access to non-law enforcement expertise and relevant information, in particular from the private sector in the area of cyber security; • Overall availability of human resources at Europol, in Member States and within authorities of cooperation partners; • Timely deployment of and operational impact by the Europol Western Balkan liaison officers; • Budget availability to directly support operational actions, including for secondary security checks in migration hotspots; • Knock-on effects regarding the implementation of the Strategic Housing Roadmap in 2019-2020 (e.g. desk sharing, satellite office space); • Adequate (human) resources in 2019 for joint investigation activities, especially in light current prospects regarding an adequate growth of Europol's workforce, seen against the increase of workload and expanding responsibilities (e.g. on-the-spot deployments, challenges as highlighted in i-OCTA, TE-SAT or other strategic reports released in 2018); • Overall limited resource funding levels affecting both operational and governance, support and administration areas; • Effective and efficient future cooperation arrangements with the law enforcement services of the UK as a key Europol partner in information sharing (in light of Brexit becoming effective in 2019); • Appropriate capabilities of Europol's cooperation partners to protect the integrity and confidentiality of information exchange and operational (analysis) data, provided by or through Europol; • Clear responsibilities and participation of other EU agencies involved in the concerned operational work.			• Foster international cooperation and identify joint activities to address common challenges in the cybercrime and cyber-enabled crime area in a unified manner (Objective A.4.3); • Promote and facilitate greater information exchange in the area of counter-terrorism and provide better and extended operational support to Member States' investigations (Objective A.5.1); • Expand the scope of the Cross Border Access to Electronic Evidence (SIRIUS) Project (A.5.2); • 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 (Objective A.5.3); • Implement the affiliation of the ATLAS Network of Special Intervention Units within the structure of Europol (A.5.4); • Contribute to the development of a common EU view on criminal analysis (A.6.1); • Strengthen Europol's capabilities to handle increasing demand for strategic analysis and deliver quality strategic reports (Objective A.6.2); • Develop Europol's capabilities in the area of travel intelligence in line with the Travel intelligence Roadmap (A.6.3); • Reinforce the provision of horizontal support to investigations by advancing the development of specialist law enforcement techniques (Objective A.6.4); • 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 (Objective A.6.5); • Continue optimising Europol's corporate functions (Objective A.7.1); • Progress towards the rationalisation and expansion of Europol's capabilities in order to accommodate the growth of the agency (Objective A.7.2); • Establish a new strategy for effective awareness raising on Europol's products and services to law enforcement stakeholders (A.7.3);

Ref. nº	Risk description (cause, event and effect)	Objective area	Response type[39]	Key Response measures
				• Engaging with Europol Liaison Bureaux, as a backbone for Europol's operational engagement, in particular through the Front Office (across all related objectives); • Member States and cooperation partners take up responsibility to submit and facilitate live investigative data flow from federal, regional and local levels to Europol and communicate the opportunities Europol can offer at national levels (across all related objectives).

Ref. n°	Risk description (cause, event and effect)	Objective area	Response type[39]	Key Response measures
02	The further development of, in particular, core systems in 2019 and the related support activities, alongside increased demand towards Europol for interoperability, connectivity and use of EU databases, may lead, in view of the implementation of the Integrated Data Management Concept which became operational with the Europol Regulation, and the decision of Europol in 2018 concerning the required evolution of the Europol Analysis System (EAS), alongside continuous staff scarcity, especially in ICT and infrastructure areas, to a critical risk profile regarding the production of deliverables on time, within budget margins and against compliance requirements, especially in light of (the): • • A paradigm shift introduced with the IDMC in the Europol Regulation, compared with the regulatory principle applied since Europol was established, i.e. access by data processing purpose, not related to processing systems defined in the regulatory founding act any longer, thus implying an overhaul of the entire information architecture of Europol's IT systems, concerning which the long-term planning and resource requirements are being identified and refined; • Continuous development of additional requirements for enhanced access and interoperability with core applications and databases at EU level, which are of direct relevance to Europol's core business (e.g. SIS, EES, ETIAS, potential EU TFTS), with a view to providing adequate support services towards MS and cooperation partners; • Increased technical support to manage access to and the handling of operational live data, resulting from elevated operational cooperation needs (by making use, for instance, of standardised information exchange and search capabilities, for instance in the area of travel intelligence); • The envisaged (gradual) implementation of future-proof 'data lake' solution concept, on the basis of a single common data repository platform (integrated data set) for all core business data, to be developed and maintained under the in-house lead of Europol; • Continuously advancing (forensic) IT capabilities especially in the area of EC3 and regarding the accredited forgery of Euro currency laboratory; • Establishment and maintenance of a new decryption platform; • Tight human resource levels in infrastructure and ICT areas (given priority staffing in the core operational business);	A.1.1 A.1.2 A.2.1 A.2.2 A.4.1 A.4.2 A.4.3 A.6.3 A.6.4 A.6.5 A.7.1 A.7.2	Reduce	• Guide business delivery by the principles of simplification, convergence and unification, thus aiming to provide a healthy starting point for the changes planned in 2019, in particular in view of the Europol Regulation being operational (impact across all objectives); • Establishment of the New Environment for Operations (NEO), making use of machine learning, artificial intelligence and state-of-the art technologies, including Europol's contribution to the implementation of the June 2017 Council conclusions on the interoperability of EU information systems (impact across all objectives); • Establishment of a dedicated IDMC implementation programme (including the appointment of a Head of Unit on a full-time basis), alongside pro-active communication on the (timeline of) deliverables under the IDMC programme as multi-year endeavour; • Advance the implementation of the new information management architecture and continue improving operational capabilities and tools by focusing on automation and modernisation (Objective A.1.1); • Advance interoperability and connectivity with information management systems at EU level to enhance information exchange (Objective A.1.2); • Broaden the information processing capabilities of Europol's Front Office (A.2.1); • Utilise the newly acquired access of Europol to the Schengen Information System (A.2.2); • Accelerate Europol's capabilities to provide support to Member States' investigations in the area of cybercrime-related EU Policy Cycle priorities 2018-2021 (Objective A.4.1); • 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.4.2); • Foster international cooperation and identify joint activities to address common challenges in the cybercrime and cyber-enabled crime area in a unified manner (Objective A.4.3);

Ref. nº	Risk description (cause, event and effect)	Objective area	Response type[39]	Key Response measures
	• Elevated audit, security as well as data protection requirements, in particular in light of heightened governance provisions in the Europol Regulation; • De-prioritised development and maintenance of non-core systems and applications in the past years (e.g. in the area of contract management); • Limited funding levels dedicated to new ICT delivery scope, in particular for core business capabilities; • Increase of costs to sustain the current ICT architecture of Europol, representing an estimated amount of 20 Million Euro expected in 2019, which accounts for more than the budget available for ICT related expenditure in 2018 (18.9 Million Euro), in particular due to necessary replacements which had to be postponed in the past to fund new initiatives, thus minimising in 2019 the delivery of new scope from the 5 Million as a specific earmark included by the European Commission for ICT expenditure for the final budget for 2019; • Expanded ICT support services in general.			• Develop Europol's capabilities in the area of travel intelligence in line with the Travel intelligence Roadmap (Objective A.6.3); • Reinforce the provision of horizontal support to investigations by advancing the development of specialist law enforcement techniques (Objective A.6.4); • Increase the provision of comprehensive financial intelligence to MS regarding money laundering and asset recovery, including possible links to other criminal areas (Objective A.6.5); • Continue optimising Europol's corporate functions (Objective A.7.1); • Progress towards the rationalisation and expansion of Europol's capabilities in order to accommodate the growth of the agency (Objective A.7.2).
03	Europol is approached by various key stakeholders, including the political level, to implement ad hoc requests. Performing the resulting tasks reduces the resources available for the achievement of the objectives for 2019. Accordingly, the implementation of the goals of the Europol Strategy 2016-2020 and strategic priorities 2020+ may be at risk.	All objectives	Reduce	• Perform robust planning as well as performance measurement processes, close monitoring of the annual work planning, based on quarterly performance reporting (across all objectives); • Operating, on a continuous basis, an organisational demand management process which contributes to the appropriate re-prioritisation within the organisational mandate and reflects the principle of an efficient and effective use of available resources, in consultation with and guidance by relevant stakeholders and assurance providers (in particular the Europol MB concerning prioritisation and resource considerations); • Ensure communication which reflects realistic ambitions and plans (all activities under A.7 'Governance, support and administration'); • Development of multi-annual strategic objectives covering the years 2020+ will commence in 2019 (Objective A.7.1); • Progress towards the rationalisation and expansion of Europol's capabilities in order to accommodate the growth of the agency (Objective A.7.2).

(2) Overview of opportunities (risks which could have a positive effect on the 2019 business planning)

Ref. nº	Risk description (cause, event and effect)	Objective area	Response type[41]	Response measures
01	The adoption of the EU Internal Security Strategy (EU ISS) 2015-2020, the European Agendas on Security and Migration, the establishment of the EU Security Union, the June 2017 Council conclusions on the interoperability of EU information systems, as well as the implementation of the Europol Regulation, the Multiannual Financial Framework (MFF) 2014-2020, including the Internal Security Fund (ISF) as well as the 2018 EU security initiatives, combined with elevated governance at EU level under the auspices of the European Commission and the EU Counter Terrorism Coordinator (EU CTC) enhance coherence, thus promoting opportunities for: • A significant increase of resources allocated in the area of internal security, recognising its importance to uphold cohesion and solidarity across the EU in times of political fragmentation; • An enhanced security architecture across the EU JHA landscape, ascribing Europol a central information hub, analysis as well as operational support role for law enforcement agencies in the EU and beyond, concerning the fight against serious and organised crime (including cybercrime, migration) and terrorism; • New enhanced operational cooperation between security services (through the CTG members) and the ECTC in particular, with a view to effectively responding to the continuously developing threat from international terrorism, in line with Article 4 of the TEU and Article 67 of the TFEU; • A framework to allow parliamentary oversight and elevated levels of transparency regarding Europol's work (including the handling of sensitive and classified information) in a controlled environment, in line with best (practice) standards adopted at national and EU levels;	All objectives	Exploit	• Implement the IDMC, resulting in an enhanced information architecture at Europol, providing for a flexible, future-proof framework to manage information flows in an efficient and effective manner, meeting highest security standards, while reflecting equitable and fit-for-purpose governance and data protection principles that allow for efficient governance mechanisms and automated data handling - in contrast to single transaction and ad hoc data management (in particular: Objective A.1.1); • Implement effective cooperation processes with EU institutions and bodies, and with external partners on the basis of Europol's External Strategy 2017-2020 (Objective A.2.3); • Utilise opportunities to facilitate greater information exchange between Europol and MS' CT competent authorities, including national security services, and relevant EU information systems (Objective A.5.1); • Consolidate the implementation of the Europol Regulation, based on strong governance, support and administration (activities under A.7 'Governance, support and administration'); • Allocation of human resources (established posts) is considered by the actors involved at EU Level based on the mandate and operational delivery, allowing for adjustments of financial programming where justified and required.

---

[41] Opportunity risk type responses are: Realise (identifying and seizing a chance to realise the concerned business objective with less resources or earlier than planned); Enhance (seizing and improving on an identified opportunity, thus achieving additional gains of relevance to more than one concerned business objective); Exploit (expanding the scope of business objectives by taking advantage of multiple benefits).

Continued from above	Exploiting the benefits of the Integrated Data Management Concept at Europol in particular from a technical perspective, to realise a balanced approach between data protection and effective, as well as efficient achievement of annual objectives and long-term strategy goals, taking due care of the trust invested by Member States and other partners regarding the secure handling of information and intelligence by Europol.	Continued from above	Continued from above	
Ref. nº	**Risk description (cause, event and effect)**	**Objective area**	**Response type**[42]	**Response measures**
02	The EU Internal Security Strategy (EU ISS) 2015-2020 and the further development of the Security Union, the maturing EU policy cycle (implementation of the EMPACT priorities of the EU SOCTA), based on direct operational funding, and the consolidation of the ECTC, the EMSC, EC3 and the Front Office services at Europol may result in a further profile and awareness boost for Europol as the key agency in the EU's internal security architecture, supported by the Europol Regulation and the organisation's leading information technology capabilities. This may also support overall cohesion and solidarity across EU Member States, given internal security being perceived as a connecting factor across Member States.	All objectives	Enhance	• Building a strong and positive culture and image is supported by all stakeholders and partners of Europol, taking part in realising a further increase of Europol's profile and awareness about the unique capabilities the organisation can offer (across all objectives); • Setting up of a Europol office in Brussels to reinforce the relationship with EU institutions and bodies in line with agreed objectives (Objective A.2.2); • Establishing a permanent funding role of operational action by Europol is promoted by Europol's stakeholders (is realised with the Europol Regulation).

---

[42] Opportunity risk type responses are: Realise (identifying and seizing a chance to realise the concerned business objective with less resources or earlier than planned); Enhance (seizing and improving on an identified opportunity, thus achieving additional gains of relevance to more than one concerned business objective); Exploit (expanding the scope of business objectives by taking advantage of multiple benefits).

Annex IX: Procurement plan 2019

1. Introduction (Legal basis and financing decision):

Procurement initiatives are implemented in line with the Europol Financial Regulation as follows:

- Article 85(1) of the Europol Financial Regulation states that: "*as regards procurement, Title V of Regulation (EU, Euratom) No 966/2012* (hereinafter referred to as the EU Financial Regulation) *and Delegated Regulation (EU) No 1268/2012* (hereinafter referred to as "the Rules of Application") *shall apply (…)[43]*".

- Article 84(2) of the EU Financial Regulation states that: "*Except in the case of appropriations which can be implemented without a basic act in accordance with point (e) of the first subparagraph of Article 54(2), the commitment of expenditure shall be preceded by a financing decision adopted by the institution or the authorities to which powers have been delegated by the institution*".

- Article 110(2) and (3) of the EU Financial Regulation states that "*The financing decision shall indicate the total amount it covers and shall contain a description of the actions to be financed. It shall specify:*

  (a) the basic act and the budget line;

  (b) the objectives pursued and the expected results;

  (c) the methods of implementation;

  (d) any additional information required by the basic act for the work programme.

  In addition, (…) the financing decision shall set out the following:

  (b) for procurement: the global budgetary envelope reserved for procurements''.

2. Rules for participation in Europol tender procedures:

Eligibility and exclusion criteria

- The tenderers must be established in an EU Member State. This implies that tenderers established in third countries (non-EU countries) do not have the right to participate in Europol tendering procedures, unless other bilateral or special international agreements in the field of public procurement grant them the right to do so. In case there is no such agreement, or the agreement does not apply to the kind of contracts put out to tender, tenderers of third countries are not entitled to participate, unless otherwise explicitly allowed in the given calls published by Europol;

- The tenderers shall not be, at the time of a contract award procedure, in one of the exclusion situations referred to in Articles 136 of the EU Financial Regulation.

Selection and award criteria

- The eligible proposals/tenders will be evaluated against the selection criteria indicated in each call. In general, there are three sets of selection criteria to be assessed which are specified on a case by case basis in each tender procedure:

    - Legal and regulatory capacity;

    - Economic and financial capacity;

---

[43] As repealed by Regulation (EU, EURATOM) 2018/1046 of the European Parliament and the Council of 18 July 2018 on the financial rules applicable to the general budget of the European Union (hereinafter referred to as the EU Financial Regulation)

- Technical and professional capacity.

- The tenders which meet the selection criteria are evaluated against the award criteria indicated in each call. In general, the award criteria require the assessment of quality and price.

3. Overview of the main procurement initiatives for year 2019:

Procurement initiatives are implemented either via existing (framework) contracts or via tender procedures on the basis of the following outsourcing financing scheme:

I. Implementation of existing framework contracts through order forms (including specific contracts) or of direct contracts;
II. Other Procurements (mainly through call for tenders under open/restricted and negotiated procedures).

A summary of the main procurement initiatives is outlined in Table 1 below. It includes generic information about the procurement initiatives planned for the year of this work programme and the ones planned and performed during the year before.

A detailed overview of the procurement initiatives for **YEAR 2019** is provided in Table 2 below. The table indicates the **number of the main contracts** (i.e. above EUR 15,000) in force in 2019 and divided into two parts:

- Part A includes administration and general services-related procurement initiatives.
- Part B includes IT-related procurement initiatives.

The table also includes the **indicative list of tender procedures** to be initiated in 2019. The list of tender procedures will be further detailed once more details on calls timing will be available.

The table does not include the following data/information:

- tender procedures below EUR 15,000;
- exceptional negotiated procedures without publication of a contract notice;
- restricted procedures to be launched under existing (published) calls for expression of interest;
- inter-institutional tender procedures launched by the EU institutions, bodies and/or agencies;
- tender procedures under framework contracts with reopening of competitions (i.e. mini competitions).

In addition, Europol will place orders for supplies, services, including IT consultancy services either under Europol framework contracts or under framework contracts resulting from inter-institutional tender procedures. These orders and the inter-institutional framework contracts are not reflected in the table below.

Interested economic operators are invited to consult regularly the Europol website for low value and middle value procedures (between EUR 15,000 and below the EU thresholds) and the Official Journal of the European Union for all tender procedures from the applicable EU thresholds (currently at EUR 144,000 for services).

Table 1: Summary of the main procurement initiatives

Table Code	Other initiatives and services	Estimated commitments in EURO						
		Total Planned value (procured)	Reviewed procured value	Total Initially Budget value (procured)	Total review value (procured)	Total review budget value[44]	Number of contracts / SLA / etc	Expected number of procurements
		2017	**2017**	**2018**	**2018**	**2019**	**2019**	**2019**
Part A	**Total Procurement (non-ICT)**	17,155,400	17,543,865	21,887,680	20,964,515	25,139,066	75	16
Part B	**Total ICT procurement**	22,110,800	22,989,664	18,725,000	23,713,503	23,424,000	75	8
Total							(150)	(24)
Parts A & B	**Total all procured budget value**	39,266,200	40,533,529	40,612,680	44,678,018	48,563,066		
% of the Europol budget for procurement initiatives		34%	35%	33%	34%	35%		

---

[44] Estimated value, subject to change.

Table 2: Overview of the main procurement initiatives for 2019

TABLE PART A - Main procurement initiatives 2019 (Non ICT-related activities)

Category	Main procurement initiatives (services, supplies/goods and other initiatives) (categorised per budget headings)	Value (in Euro)	Contracts		Tenders
			Number of main contracts valid in 2019	Type of contracts	Number of tenders to be initiated by EUROPOL
Category A1	Staff-related expenditure, excluding salaries or allowances (medical services, training, etc.)	4,674,166	22	FWC Direct Other	7
Category A2	Building-related expenditure (e.g. rent, energy, cleaning, maintenance, furniture, security, hospitality, etc.)	10,807,200	20	FWC Direct Other	3
Category A3	Administrative –related expenditure (e.g. postal services, stationary, open source, library, catering, insurance, publication, uniform, legal, PR items, etc.)	2,239,900	28	FWC Direct	5
Category A4	Meeting-related expenditure (e.g. travel, Hotels, interpretations, Translations, meetings)	7,417,800	5	FWC Other	1
Sub-Total Category A		**25,139,066**	**75**		**16**

No	Type of Procurement initiatives (as divided in accordance with table above)	Subject	Estimated budget in Euro[45]	Indicative timeframe		Comments
				Indicative time frame for tender initiation	Indicative time frame for tender completion	
1	Category A1	**Medical and Occupational Health and Safety services (and medical supplies)**	Above EU threshold (around 2,500,000 out of 4 years)	Q4.2019	Q3.2020	Existing Contract expiry date: 26.09.2020
2	Category A1	**Language training for staff**	Above EU threshold (around 400,000 out of 4 years)	Q2.2019	Q3.2019	New initiative (from 2018 tender planning)
3	Category A1	**General competences personal training**	Above EU threshold (around 200,000 out of 4 years)	Q2.2019	Q3.2019	New initiative From 2018 tender planning - (tentative - depending on the outcome of an inter-institutional procedure)
4	Category A1	**Psychological support services**	Below EU threshold (around 80,000 out of 1 year)	Q1.2019	Q3.2019	New initiative
5	Category A1	**Training and external expertise for the Operations Department**	Below EU threshold (around 134,000 out of 1 year)	Q1.2019	Q4.2019	Recurrent need - use of CEI list or ad hoc procedures including: - use of experts/speakers - training for Directorate Operations Staff
6	Category A1	**Training for Europol's security officers**	Below EU threshold (around 25,000 out of 1 years)	Q3.2019	Q4.2019	Recurrent needs
7	Category A1	**Annual Training courses for the Cyber Crime Center (EC3)**	Below EU threshold (around 90,000 out of 1 year)	Q1.2019	Q2.2019	Existing Contracts expiry date: Third quarter 2018
8	Category A2	**EMAS registration audit services**	Below EU threshold (around 30,000 out of 1 year)	Q4.2019	Q2.2020	New initiative

The table above is headed: **Tentative detailed overview of tender procedures (non-IT sector) to be initiated in 2019**

[45] Estimated amounts provided for information only where available. Below EU threshold = below EUR 135,000; Above EU threshold = above EUR 135,000.

9	Category A2	**Security Guards services**	Above EU threshold (around 1,000,000 out of 4 years)	Q2.2019	Q4.2019	Existing Contract expiry date: 04.01.2020
10	Category A2	**Hospitality, Conference and related services**	Above EU threshold (around 1,800,000 out of 4 years)	Q1 2019	Q2.2019	From 2018 tender planning - Existing Contract expiry date: 26.06.2019
11	Category A3	**Uniforms for security guards, staff and deployed personnel**	Above EU threshold (around 200,000 out of 4 years)	Q3.2019	Q1.2020	One existing Contract expiry date: 25.07.2021 (for security guards uniforms only)
12	Category A3	**Periodicals and databases services**	Above EU threshold (around 5,000,000 out of 4 years)	Q1.2019	Q3.2019	One existing inter-institutional contract but budget ceiling insufficient to cover Europol's needs
13	Category A3	**Furniture and other acquisitions**	Above EU threshold (around 3,500,000 out of 4 years)	Q1.2019	Q3.2019	From 2018 tender planning - Existing Contract expiry date: 25.06.2019
14	Category A3	**Consultancy services for Local Staff Pension fund closure and Dutch pension funds**	Below EU threshold (around 60,000 out of 1 year)	Q3.2019	Q4.2019	From 2018 tender planning
15	Category A3	**Acquisition or Leasing of Europol duty cars**	Below EU threshold (around 135,000 out of 4 years)	Q2.2019	Q3/Q4.2019	New initiative (tentative - depending on the outcome of an interinstitutional procedure)
16	Category A4	**Travel services**	Above EU threshold (around 400,000* out of 4 years) * travel tickets value not included	Q3.2019	Q1.2020	Existing Contracts expiry date: 15.02.2020 (tentative - depending on the outcome of interinstitutional procedure 02/PR/2017/073)

TABLE PART B - Main procurement initiatives 2019 (ICT-related activities)

Category	Main procurement initiatives (services, supplies/goods and other initiatives) (categorised per budget headings)	Value (in Euro)	Contracts[46]		Tenders
			Nr of main contracts valid in 2019	Type of contracts	Nr of tenders to be initiated by EUROPOL
Category B1	Administrative purchase and maintenance of Hardware and Software	800,000	18	FWC	
Category B2	Administrative ICT studies and strategic consultancy services	134,000	6	FWC	
Category B3	Administrative ICT External Service Provision including development and maintenance of solutions	850,000	12	FWC	1
Category B4	Administrative Telecommunications costs	750,000	6	FWC	2
Category B5	Operational training	154,000	1	FWC	1
Category B6	Operational purchase and maintenance of Hardware and Software	10,886,000	18	FWC	1
Category B7	Operational ICT External Service provision including development and maintenance of solutions	8,500,000	12	FWC	3
Category B8	Other telecommunications costs incl. management of network to MS	1,350,000	2	FWC	
Sub-Total Category B		**23,424,000**	**75**		**8**

---

[46] A contract may cover several categories and be counted more than once.

No				Tentative detailed overview of IT-related tender procedures to be initiated in 2019:		
				Indicative timeframe		
	Category	**Subject**	**Estimated budget**[47]	**Indicative time frame for tender initiation**	**Indicative time frame for tender completion**	**Comments**
17	Category B3	**Acquisition channel for ICT Security Systems**	Below EU threshold (around 10,000,000 out of 4 years)	Q4.2019 Q1.2020	Q4.2020	One existing Contract expiry date: 30.01.2021
18	Category B4	**Fixed Telephony Services**	Above EU threshold (around 1,300,000 out of 4 years)	Q4.2019	Q2.2020	One existing Contract expiry date: 03.06.2020
19	Category B4	**Mobile Telephony Services**	Above EU threshold (around 4,500,000 out of 4 years)	Q4.2018/Q1.2019	Q2.2019	One existing Contract expiry date: 06.2020
20	Category A1	**Acquisition channel for IT training courses**	Above EU threshold (around 1,300,000 out of 4 years)	Q1.2019	Q3.2019	One existing Contract expiry date: 18.02.2020
21	Category B6	**Provision of Replacement Encryptors and related services**	Above EU threshold (around 6,000,000 out of 4 years)	Q1.2019	Q3.2019	Existing Contract expiry date: 11.09.2019 (From 2018 tender planning)
22	Category B7	**ICT Consultancy Services, including software factory services**	Above EU threshold (around 25,000,000 out of 4 years)	Q1.2019	Q3.2019	Existing Contract expiry date: several contracts LOT 1: 03/12/2019 LOT 2: 09/09/2019 LOT 3: 10/01/2020 LOT 4: 16/12/2019
23	Category B7	**Service Desk and ICT Business Support**	Above EU threshold (around 1,000,000 out of 4 years)	Q1.2019 (launched date to be postponed to Q3.2019 if not included in tender nbr	Q3.2019	Existing Contract expiry date: 26.07.2020 (Tentative - specific profile/expertise to be merged with ICT Consultancy)
24	Category B7	**Consultancy services on Specialised Software**	Above EU threshold (around 1,000,000 out of 4 years)	Q1.2019	Q3.2019	New Initiative (tentative - specific profile/expertise to be merged with ICT Consultancy)

[47] Below EU threshold = below EUR 135,000; Above EU threshold = above EUR 135,000.

Annex X: Grants 2019

1. Restricted call for proposals to support the implementation of activities identified by the Council

Legal basis:

> Article 4 and Article 61 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.
>
> Council conclusions on setting the EU's Priorities for the fight against organised and serious international crime between 2018 and 2021, doc. 9450/17 COSI 107 of 19 May 2017.

Budget line

> To be defined

Priorities of the year, objectives pursued and expected results

> Enhancing the fight against serious and organised international crime during the second year of the implementation of the EU Policy Cycle 2018-2021.
>
> The call is restricted to EMPACT participants and it is announced on Europol website, while all relevant documents are published on the Europol Platform for Experts – a communication tool with EMPACT participants used to reach all potential applicants. In accordance with Europol legal basis, the Europol national unit (ENU) shall be the liaison body between Europol and the competent authorities of the Member States. Thus, the applications must always be submitted via the ENU of the Lead Applicant.
>
> The objective of the call is to provide support to Operational Actions laid down in the thirteen Operational Action Plans (OAPs) as adopted by the Council. In the current EU Policy Cycle the OAPs address the following crime areas: Cybercrime: (i) Attacks against Information Systems, (ii) Child Sexual Exploitation and (iii) Non-cash payment fraud; Cannabis, Cocaine and Heroin; New Psychoactive Substances and Synthetic Drugs; Facilitated Illegal Immigration; Organised property crime; Trafficking in Human Beings (THB); Excise Fraud; MTIC Fraud; Firearms; Environmental crime; Criminal finances, money laundering and asset recovery; and Document fraud[48].
>
> It is expected that the support will provide for improved cooperation between Member States law enforcement agencies, EU Institutions, EU Agencies and relevant third parties while delivering coherent actions targeting the most pressing criminal threats facing the EU.

Description of the activities to be funded under the call for proposals

> Transnational operational and non-operational activities addressing in each of the EMPACT Priorities at least one of the following objectives: awareness raising and exchange of best practices; improving data gathering and intelligence sharing, providing strategic support for current or proposed operational activities; enhancing operational support and cross-border cooperation.
>
> Calls will be designed with the aim of promoting one or more of the following outcomes which projects applications should aim at achieving:
> - fostering communication and coordination amongst participants of OAPs;
> - sharing of experiences and best practices between EU Member States;
> - improving intelligence gathering and analyses;

---

[48] Document fraud is a cross-cutting crime priority without a dedicated OAP.

- expanding data sharing with Europol information systems and prioritising the use of SIENA (secure line) as an operational communication tool;
- establishing support frameworks to implement operational activities, including where relevant with third countries or the private sector;
- enhancing cross-border/transnational operational cooperation between EU Member States and, where relevant, with third countries or the private sector;
- establishing joint investigations, joint operations or joint action days.

Europol may award using simplified cost options provided that a decision by the Executive Director has been adopted.

Essential eligibility, selection and award criteria

Eligibility criteria:
I. In order to be eligible the Applicant must be a public body established in an EU Member State participating in the OAP in question (i.e. the particular EMPACT crime priority) and in the law-enforcement cooperation under Europol Regulation.
II. The Co-Applicants must be:
• An entity explicitly mentioned as a participant in the OAP;
• If the entity is not explicitly mentioned in the OAP, any of the following entities may be Co-Applicants, provided their participation is justified by the nature of the action:
- A public body established in an EU Member State or in a third country OR
- A profit or non-profit-oriented organisation established in an EU Member State or in a third country, OR
- An International Organisation.

III. Applications must involve at least two (2) public bodies established in two (2) different EU Member States.

IV. The proposed activities must be mentioned in the respective OAPs as approved by COSI Council decisions.

Selection criteria:
In accordance with Article 198 of the Financial Regulation, proposals for action shall be evaluated on the basis of the following selection criteria:
- Financial capacity - Applicants and co-applicants must have stable and sufficient sources of funding to maintain their activity throughout the period during which the activity is being carried out and to participate in its funding.
- Operational capacity - Applicants and co-applicants must have the professional resources, competences and qualifications required to complete the proposed action.
The verification of the financial and operational capacity shall not apply to public bodies and international organisations in accordance with Article198) of the Financial Regulation.

Award criteria:
In accordance with Article 199 of the Financial Regulation, proposals for an action shall be evaluated on the basis of the relevance, quality, cost-effectiveness and European added value of the proposed action.

Indicative timetable and indicative amount of the call for proposals

Date	Amount
Publication: Q4 year N-1 Award of grants: Q1 year N	EUR 3 million

Maximum possible rate of co-financing of the total eligible costs

95%

2. **Open-ended restricted Call for Proposals for ad-hoc low-value grants in support of operational activities as laid down in the Operational Action Plans implementing the EU Policy Cycle for Serious and Organised Crime.**

Legal basis

Article 4 and Article 61 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

Council conclusions on setting the EU's Priorities for the fight against organised and serious international crime between 2018 and 2021, doc. 9450/17 COSI 107 of 19 May 2017.

Budget line

To be defined

Priorities of the year, objectives pursued and expected results

Enhancing the fight against serious and organised international crime during the second year of the implementation of the EU Policy Cycle 2018-2021.

The objective of the low-value grants is to provide support tailored to operational activities within the thirteen Operational Action Plans (OAPs) adopted by the Council. They target activities that are developed on an ad-hoc basis rather than as a result of a long-term planning, due to their investigative nature or other quickly changing aspects of crime phenomena and crime-countering measures. In the current EU Policy Cycle the OAPs address the following areas: Cybercrime: (i) Attacks against Information Systems, (ii) Child Sexual Exploitation and (iii) Non-cash payment fraud; Cannabis, Cocaine and Heroin; New Psychoactive Substances and Synthetic Drugs; Facilitated Illegal Immigration; Organised property crime; Trafficking in Human Beings (THB); Excise Fraud; MTIC Fraud; Firearms; Environmental crime; Criminal finances, money laundering and asset recovery; and Document fraud.

It is expected that the support will provide for effective cooperation between Member States law enforcement agencies, EU Institutions, EU Agencies and relevant third parties while delivering coherent operational actions targeting the most pressing criminal threats facing the EU. The funded measures should achieve concrete, quantifiable / measurable operational results.

Description of the activities to be funded through low-value grants

Transnational short-term operational and/or investigative activities within the EMPACT Priorities, with a budget not exceeding 60,000 EUR (in line with the threshold defined in the EU Financial Regulation), aiming to enhance operational cross-border cooperation, establish joint investigations, joint operations or joint action days.

Europol may use simplified cost options provided that a decision by the Executive Director has been adopted.

Essential eligibility, selection and award criteria

Eligibility criteria:
I. In order to be eligible the Applicant must be a public body established in an EU Member state participating in the OAP in question (i.e. the particular EMPACT crime priority) and in the law-enforcement cooperation under Europol Regulation.
II. The Co-Applicants must be:
• An entity explicitly mentioned as a participant in the OAP;
• If the entity is not explicitly mentioned in the OAP, any of the following entities may be Co-Applicants, provided their participation is justified by the nature of the action:

- A public body established in an EU Member State or in a third country OR
- A profit or non-profit-oriented organisation established in an EU Member State or in a third country, OR
- An International Organisation.

III. Applications must involve at least two (2) public bodies established in two (2) different EU Member States.

IV. The proposed activities must be mentioned in the respective OAPs as approved by COSI Council decisions.

V. The requested grant cannot be higher than 60,000 EUR, or in line with the current threshold for low-value grants established by the EU Financial Regulation.

Selection criteria:
In accordance with Article 198 of the Financial proposals for action shall be evaluated on the basis of the following selection criteria:
- Financial capacity - Applicants and co-applicants must have stable and sufficient sources of funding to maintain their activity throughout the period during which the activity is being carried out and to participate in its funding.
- Operational capacity - Applicants and co-applicants must have the professional resources, competences and qualifications required to complete the proposed action.
- The verification of the financial and operational capacity shall not apply to public bodies and international organisations in accordance with Article 198 of the Financial Regulation.

Award criteria:
In accordance with Article 199 of the Financial Regulation proposals for an action shall be evaluated on the basis of the relevance, quality, cost-effectiveness and European added value of the proposed action.

Indicative timetable and indicative amount of the call for proposals

Date	Amount
Publication: Q1 year N Award of grants: Q1-Q4 year N	EUR 1 million

Maximum possible rate of co-financing of the total eligible costs

95%

3. Support for combatting Euro-counterfeiting

Legal basis

Article 4(4) and Article 61 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

Budget line

To be defined

Priorities of the year, objectives pursued and expected results

Operational actions and support for coordination activities within the guidelines approved by the Europol Management Board with the objective of protecting the euro currency from counterfeiting activities.

Description of the activities to be funded through low-value grants

Applications submitted must involve at least one of the following activities, all designed with the objective of protecting the integrity of the Euro currency:

- Investigations into or related to euro counterfeiting. This means inquiries related to counterfeit euro banknotes and counterfeit euro coins, as well as the production and the distribution of them;
- Technical investigations using forensic and/or scientific analysis to identify, sites, raw materials and technical equipment used for the production of counterfeit euro notes and coins as well as measures to locate technical equipment used;
- Investigative measures carried out in compliance with the applicable national law and in accordance with these guidelines;
- Operational or technical investigations into euro counterfeiting involving cooperation with third countries.

In addition, the applicant must commit to a degree of involvement of Europol:
- as a minimum to ensure the role of Europol as the Central Office, the law enforcement information, including samples of any counterfeit currency recovered, must be shared with Europol via the appropriate channels;
- on the spot support where an application involves a production site(s).

Essential eligibility, selection and award criteria
This is not a general advertised call due to the restricted pool of potential beneficiaries. The possibility and funds available shall be made known to the entities foreseen under the Europol Management Board approved rules.

Indicative amount available

Date	Amount
Q1-Q4	100,000 + internal assigned revenue[49]

Maximum possible rate of co-financing of the total eligible costs

100% maximum

4. ATLAS Network grant

Legal basis:

Article 4(1)(h) and (i) and Article 61(3) of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.Terms of Reference signed between Europol, Atlas Chair and Austrian Ministry of Interior and entering into force on 10 October 2018.

Budget line

To be defined. The budget has not currently been made available in the draft budget for 2019. Atlas activities are currently funded by the Commission as part of its ISF grant programme until June 2019. The Terms of Reference referred to above foresaw the transfer of funding from this point to Europol provided that resources were made available. No resources were made available to Europol in 2019 for Atlas funding.   Europol and the Commission are aware of the budgetary needs. According to the Terms of Reference, support for Atlas is conditional upon sufficient funding to be available to ensure that Europol's core activities are not affected.

Priorities of the year, objectives pursued and expected results

---

[49] as mentioned in the guidelines EDOC #878276

The ATLAS Network is a cooperation structure between 38 Special Intervention Units (SIUs).

The main priority for the year 2019 is the execution of cross border operations and training.

Description of the activities to be funded under the call for proposals

Depending on the level of funding made available, and the timing of the finalisation of funding under the ISF programme, Europol would consider making one grant or smaller grant awards using a fast track procedure as employed and described for EMPACT. The priorities and objectives shall also take into account the need to avoid double funding.

The activities, dependent on budget availability, are:-
- fostering communication and coordination amongst SIUs, operational training and first aid training;
- sharing of experiences and best practices between EU Member States;
- establishing support frameworks to implement operational activities;
- enhancing cross-border/transnational operational cooperation between EU Member States in the areas of competence of SIUs;
- establishing joint training and preparation for challenges impacting on several Member States; and
- evaluation of training and cooperation results.

Europol may award using simplified cost options provided that a decision by the Executive Director has been adopted.

Justification Direct Grant

Under Article 61(3) of the Europol Regulation, the grant (or grants) may be awarded without a call for proposals where the grant action is supporting specific tasks referred to in points (h) and (i) of Article 4(1) of the Europol Regulation. As illustrated above by the description of the objectives, results and actions, this grant indeed provides funds to the Atlas network (via the legal entity of the country chairing Atlas on behalf of the network) involves the use the grant funding for performance of cross-border operations and investigations and for the provision of training.

Indicative timetable and indicative amount of the call for proposals

Date	Amount
Q3	Tbc

Maximum possible rate of co-financing of the total eligible costs

95%

Europol Public Information

Annex XI:
Organisation chart

Europol Public Information