EN

THIS ACTION IS FUNDED BY THE EUROPEAN UNION

ANNEX V

to the Commission Implementing Decision on the financing of the 2023 action plan part II in favour of the Regional South Neighbourhood

Action Document for 2023 Security Package

ANNUAL ACTION PLAN
This document constitutes the annual work programme in the sense of Article 110(2) of the Financial Regulation, and action plan/measure in the sense of Article 23(2) of NDICI-Global Europe Regulation.

1. SYNOPSIS

1.1. Action Summary Table

1. Title **OPSYS** **Basic Act**	2023 Security Package 2023 annual action plan part II in favour of the Regional South Neighbourhood OPSYS business reference: ACT-61717 ABAC Commitment level 1 number: JAD.1158403 Financed under the Neighbourhood, Development and International Cooperation Instrument (NDICI-Global Europe)
2. Economic and Investment Plan (EIP)	Yes
EIP Flagship	FLAGSHIP 7 – Digital transformation, research and innovation
3. Team Europe Initiative	No
4. Beneficiar(y)/(ies) of the action	The action shall be carried out in the Neighbourhood South countries: Algeria, Egypt, Israel ([1]), Jordan, Lebanon, Libya, Morocco, Palestine ([2]), Syria ([3]) and Tunisia. As per Article 43(1) of NDICI-Global Europe Regulation, for reasons of efficiency and effectiveness, and upon explicit justified request, some activities may be

[1] See Guidelines on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards on http://eurlex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2013.205.01.0009.01.ENG.

[2] This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the Member States on this issue.

[3] Co-operation with the Government of Syria suspended since 2011.

	extended to countries from the Union for the Mediterranean and countries neighbouring Neighbourhood South countries: Albania, Bosnia and Herzegovina, Mauritania, Montenegro, North Macedonia, Türkiye, Chad, Mali, Niger, Saudi Arabia, Sudan and Iraq. This is justified because the action intervenes in the field of security, which has transboundary effects and may be enhanced by cross-regional sharing of best practices. It is in line with the Multi-annual indicative programme for the Southern Neighbourhood for 2021-2027, which makes reference, under priority 5 (specific objective 2) to the importance of cross regional cooperation.[4]
5. Programming document	Multi-annual indicative programme for the Southern Neighbourhood (2021-2027)[5]
6. Link with relevant MIP(s) objectives/expected results	Priority area 3: "Peace and Security" SO1: Strengthen cooperation to fight organised crime and terrorism between partner countries and with EU Member States SO2: Improving judicial cooperation in civil matters
PRIORITY AREAS AND SECTOR INFORMATION	
7. Priority Area(s), sectors	151 Government and Civil Society-General 152 Conflict, Peace and Security
8. Sustainable Development Goals (SDGs)	Main SDG (1 only): SDG 16: Peace, Justice and Strong Institutions Other significant SDGs (up to 9) and where appropriate, targets: SDG 9: Industry, innovation and infrastructure
9. DAC code(s)	15130 - Legal and judicial development 50 % 15210 - Security system management and reform 50%
10. Main Delivery Channel @	40000 - Multilateral Organisation 47138 – Council of Europe 10000 - Public Sector Institutions
11. Targets	☐ Migration ☐ Climate ☐ Social inclusion and Human Development ☒ Gender ☐ Biodiversity ☒ Human Rights, Democracy and Governance

12. Markers (from DAC form)	**General policy objective @**	**Not targeted**	**Significant objective**	**Principal objective**

[4] "The future regional cooperation should have a flexible geographical and thematic scope, also allowing for interlinkages with other regions, where necessary and appropriate as highlighted in the Joint Communication on a Renewed partnership with the Southern Neighbourhood."

[5] C(2021) 9399 Commission Implementing Decision for the adoption of a Multiannual Indicative Programme (MIP) in favour of the Southern Neighbourhood for the period 2021-2027

	Participation development/good governance	☐	☐	☒
	Aid to environment @	☒	☐	☐
	Gender equality and women's and girl's empowerment	☒	☐	☐
	Reproductive, maternal, new-born and child health	☒	☐	☐
	Disaster Risk Reduction @	☒	☐	☐
	Inclusion of persons with Disabilities	☒	☐	☐
	Nutrition @	☒	☐	☐
	RIO Convention markers @	**Not targeted**	**Significant objective**	**Principal objective**
	Biological diversity @	☒	☐	☐
	Combat desertification @	☒	☐	☐
	Climate change mitigation @	☒	☐	☐
	Climate change adaptation @	☒	☐	☐
13. Internal markers and Tags	**Policy objectives**	**Not targeted**	**Significant objective**	**Principal objective**
	EIP	☐	☒	☐
	EIP Flagship	YES ☒		NO ☐
	Tags transport energy environment, climate resilience digital economic development (incl. private sector, trade and macroeconomic support) human development (incl. human capital and youth) health resilience migration and mobility other	YES ☐ ☐ ☐ ☒ ☐ ☐ ☐ ☐ ☐		NO ☒ ☒ ☒ ☐ ☒ ☒ ☒ ☒ ☒
	Digitalisation @	☐	☒	☐
	Tags digital connectivity	YES ☐		NO ☒

digital governance	☒		☐
digital entrepreneurship	☐		☒
digital skills/literacy	☐		☒
digital services	☐		☒
Connectivity @	☒	☐	☐
Tags	YES		NO
digital connectivity	☐		☒
energy	☐		☒
transport	☐		☒
health	☐		☒
education and research	☐		☒
Migration@	☒	☐	☐
Reduction of Inequalities @	☒	☐	☐
COVID-19	☒	☐	☐

BUDGET INFORMATION	
14. Amounts concerned	Budget line(s) (article, item): 14.020110 Southern Neighbourhood Total estimated cost: EUR 9 850 000 Total amount of EU budget contribution: EUR 9 500 000
MANAGEMENT AND IMPLEMENTATION	
15. Implementation modalities (management mode and delivery methods)	**Indirect management** with the Council of Europe and the European Union Agency for Law Enforcement Training (CEPOL)

1.2. Summary of the Action

The present action which reflects the EU priorities under the Joint Communication on a Renewed Partnership with the Southern Neighbourhood[6] and its Economic and Investment Plan (EIP)[7]. The objectives of the action are also aligned with the Union for the Mediterranean (UfM) political framework. This action implements the Multi-Annual Indicative Programme for the Southern Neighbourhood (2021-2027)[8] under its Priority Area 3 "Peace and Security". It contributes to the EIP flagship 7 "Digital transformation, research and innovation".

Component 1: Euromed Police VI:

The first component, **Euromed Police**, will further develop the concept of a sustainable cooperation mechanism for cross-border police cooperation in criminal matters, between EU Member States and the

[6] JOIN (2021) 2 final of 09.02.2021
[7] SWD(2021) 23 final
[8] C(2021) 9399 final

Southern Partner Countries (SPCs) with a more direct involvement of EU Justice and Home Affairs agencies (namely CEPOL, and Europol). Building on the achievements of the previous editions of the project, this sixth phase of Euromed Police will contribute to further expand the external dimension of the EMPACT-cycle in the Southern Neighbourhood region to address the common challenges of organised crime. The project will develop the concept of an EMPACT support network, to foster the multidisciplinary approach towards the fight against organised crime. It will also further promote regional coordination by integrating Southern Partner Countries within the analysts' community through Europol's Platform for Experts.

This component prioritises the fight against organised crime, in support of the EU Strategy to tackle Organised Crime 2021-2025. It focuses on strengthening cooperation in order to effectively fight organised crime and terrorism, as specified in the related specific objective 3.1 of the multi-annual indicative programme for the Southern Neighbourhood. This component is framed within the context of SDG 16 (Peace, Justice and Strong Institutions), promoting peaceful and inclusive societies grounded in human rights and the rule of law.

Component 2: CyberSouth +

CyberSouth+ will aim at strengthening criminal justice capacities for enhanced cooperation on cybercrime and disclosure of electronic evidence through a combination of regional and country-specific actions that will be tailored to the needs and capacities of each project country. While CyberSouth+ will build upon the achievements of the CyberSouth project, this new phase will continue to support the reform of domestic legislation in line with the Budapest Convention on Cybercrime. The support will be extended to the alignment with the Second Additional Protocol on electronic evidence and the convention 108+ on personal data protection. This project will also contribute to greater synergies between criminal justice and cybersecurity responses to cyber threats, by supporting mechanisms for trusted cooperation and reporting between cybersecurity institutions and criminal justice authorities. Finally, the geographical scope of the project will be extended to cover the entire Southern Neighbourhood region.

This component prioritises the fight against cybercrime and relates to the specific objective 3.1 of the multi-annual indicative programme for the Southern Neighbourhood. This component is framed within the context of SDG 16 (Peace, Justice and Strong Institutions), promoting peaceful and inclusive societies grounded in human rights and the rule of law.

1.3. Beneficiar(y)/(ies) of the action

The two components of this Action shall be carried out in the Neighbourhood South countries: Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine, Syria[9] and Tunisia out of which only Israel is not included in the list of ODA recipients.

The two components of this Action are of regional nature, fostering regional cooperation. Due to the project's nature and the importance to ensure extended regional coverage, the eligibility of the action could be extended exceptionally to the following countries or territories, as their participation could constitute a substantial element to ensure the coherence and effectiveness of Union financing or to foster regional or trans-regional cooperation: countries from the Union for the Mediterranean and countries neighbouring Neighbourhood South countries: Albania, Bosnia and Herzegovina, Mauritania, Montenegro, Türkiye, Chad, Mali, Niger, Saudi Arabia, Sudan and Iraq.

[9] Cooperation with Syria is temporary suspended.

2. RATIONALE

2.1 Context

Euromed Police VI:

This component prioritises the fight against organised crime, in support of the EU Strategy to tackle Organised Crime 2021-2025. It focuses on strengthening cooperation between South Partner Countries (SPCs) and with EU Member States in order to effectively fight organised crime and terrorism, as specified in the related specific objective 3.1 of the multi-annual indicative programme for the Southern Neighbourhood.

The EU has reinforced its actions against organised crime by adopting a comprehensive Security Union Strategy in 2020 and follow up strategies on organised crime, and on specific crime areas including drugs, firearms trafficking and trafficking in human beings. These strategies have a strong external dimension encouraging international cooperation, including with countries of the Neighbourhood Policy. Moreover, the Council of the European Union agreed on the priorities for the European Multidisciplinary Platform Against Criminal Threats (EMPACT) for 2022-2025 on the basis of the latest European Union Serious Organised Crime Threat Assessment (EU SOCTA) published in April 2021 by Europol. Trafficking in drugs, firearms, and human beings, as well as cybercrime, remain high priorities.

The EU recognises the global character of organised crime and the importance of further intensifying and improving cooperation and association with third countries and relevant international organisations in the operational implementation of EMPACT, including support for the possible development of an "EMPACT methodology" outside the EU.

The fifth phase of Euromed Police has been contributing to this general approach. The transfer of the project to CEPOL and Europol represented a new step towards an EU coordinated approach for the South Partner Countries. The project successfully integrated the EMPACT community in the delivery of some of the activities (training activities on crime priorities and strategic cooperation forums), which is a first step towards a coordinated operational approach in the fight against organised crime. The sixth phase of Euromed Police will pursue this approach and further develop the "EMPACT methodology".

CyberSouth +

This component prioritises the fight against cybercrime, in support of the 2020 Security Union Strategy, the 2020 EU Cybersecurity Strategy and the EU Strategy to tackle Organised Crime 2021-2025. It focuses on strengthening legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighbourhood in line with human rights and rule of law requirements. This component responds to the specific objective 3.1 of the multi-annual indicative programme for the Southern Neighbourhood and to flagship 7 - *Digital transformation, research and innovation* -of the Economic and Investment Plan (EIP).

Cybercrime is a global challenge where effective international cooperation is necessary. The EU supports the Council of Europe's Budapest Convention on cybercrime, which is an effective, well-established framework that allows all countries to identify what systems and communication channels they need to put in place to be able to work effectively with each other. Morocco is a Party to the Convention. Tunisia was invited to become a Party to the Budapest Convention in 2018. The country requested an additional year to the 5-year term to adhere to the Convention. The additional year was granted and the new deadline for ratification is now set for February 2024. Algeria, Jordan and Lebanon have adopted legislation that is partially in line with the Budapest Convention and that would require – to different extents - further

interventions to strengthen safeguards and provisions on international co-operation. Egypt, Libya and Palestine have also adopted cybercrime legislation which would require further work to comply with international rule of law standards.

While cybercrime is proliferating, the complexity of obtaining electronic evidence stored in foreign or unknown jurisdictions is increasing and limiting the power of law enforcement to their territorial boundaries. Indeed, the transfer of electronic evidence from one state to another requires the processing of personal data of parties to criminal cases. While for the EU Member States, data protection standards in criminal procedures are established in a common and similar manner at EU level, for the countries from Middle East and North Africa, the data protection legal frameworks differ from one country to another. EU Member States and South Partner Countries criminal justice authorities are not always familiar with the legal systems and the data protection requirements existing in the countries from the opposite shore of the Mediterranean and this negatively affects the cross-regional judicial cooperation. As a result, only a very small number of cybercrimes are prosecuted.

The new Second Additional Protocol to the Budapest Convention aims to respond to this challenge by providing tools for enhanced co-operation and disclosure of electronic evidence - such as direct cooperation with service providers. Morocco was among the first signatories of the Second Additional Protocol in May 2022. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) is another tool at the disposal of South Partner Countries. It is the first legally binding international instrument in the data protection field. Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data. Tunisia and Morocco have respectively ratified the Convention 108 in 2017 and 2019, not yet the modernised Convention 108+
The Council of Europe and the European Union have been supporting Algeria, Jordan, Lebanon, Morocco and Tunisia since 2017 through the joint project CyberSouth aimed at strengthening "legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighbourhood."[10]

With CyberSouth coming to an end in December 2023, a follow up joint project CyberSouth+ is proposed.
CyberSouth+ will aim at strengthening criminal justice capacities for enhanced cooperation on cybercrime and disclosure of electronic evidence through a combination of regional and country-specific actions that will be tailored to the needs and capacities of each project country. While CyberSouth+ will build upon the achievements of the CyberSouth project, this new phase will continue to support the reform of domestic legislation in line with the Budapest Convention on Cybercrime. The support will be extended to the alignment with the Second Additional Protocol on electronic evidence. This project will also contribute to greater synergies between criminal justice and cybersecurity responses to cyber threats, by supporting mechanisms for trusted cooperation and reporting between cybersecurity institutions and criminal justice authorities. Finally, the geographical scope of the project will be extended to cover the entire Southern Neighbourhood region, including Egypt, Libya and Palestine.

2.2. Problem Analysis

Short problem analysis

[10] C(2016)4858 Commission implementing Decision on the Annual Action Programme 2016 – Part 1 in favour of the ENI South countries to be financed from the general budget of the European Union

Euromed Police VI

Southern Neighbourhood countries remain points of origin, transit and destination for a multitude of trafficking. According to the latest Global Organized Crime Index[11], organised crime in pervasive in North Africa and the Middle East. The most prevalent crimes in the region are human smuggling and trafficking in human beings. Libya remains a major transit hub from migrants being smuggled from across Africa, but experts identified Tunisia as an emerging significant source country for irregular migration to Italy. Drugs and arms trafficking are also widespread. Libya is ranked as the worst country in the world for arms trafficking; while Morocco and Lebanon's criminal markets for the illicit cultivation, distribution and sale of cannabis are some of the largest in the world.

Organised criminal groups are increasingly active across criminal markets (drugs, arms, wildlife trafficking, among others) and ready to adapt their methods to circumstances, highlighting the need for law enforcement response to be agile, swift and coordinated. Serious and organised crime is also becoming more and more trans-regional. It represents a shared challenge for both shores of the Mediterranean. Strengthening strategic and operational police cooperation within the Southern Partner Countries and also with the EU is therefore paramount. Strengthening cooperation on common threats and objectives has been persistently increasing among Southern Partner Countries and a number of EU Member States. Tackling serious and organised crime requires that regional cooperation mechanisms be strengthened, starting from a shared threat assessment based on joint analysis.

CyberSouth+:

Countries of the Southern Mediterranean region – as societies all over the world – increasingly rely on information and communication technologies (ICT) and are therefore vulnerable to threats such as cybercrime. Cybercrime – that is offences against computer systems and by means of computers – affects individuals, institutions and organisations as well as States. According to the 2022 INTERPOL Global Crime Trend Report, computer intrusion, phishing, online scams, and ransomware are the cybercrime trends, which MENA countries most frequently perceived as 'high' threats.

Cybercrime is a trans-national threat. Justice and law enforcement authorities are increasingly dependent on electronic evidence, which may be located in foreign jurisdiction. Making it easier and quicker to obtain this evidence across borders is of crucial importance for investigating and prosecuting crime, but also more generally for strengthening the law enforcement apparatus. The transfer of electronic evidence from one state to another also requires the consideration of other parameters, as it implies the processing of personal data. Legal systems and data protection requirements differ between countries and may negatively affect cross-regional judicial cooperation.

Finally, the growing number of attacks against critical information infrastructure underline the need for synergies between criminal justice responses to cybercrime and measures to enhance cybersecurity. Gathering electronic evidence as soon as possible and before remediation remains essential for successful investigations. Law enforcement and the cybersecurity community should cooperate closely to ensure a collective and comprehensive response.

Identification of main stakeholders and corresponding institutional and/or organisational issues (mandates, potential roles, and capacities) to be covered by the action.

[11] https://ocindex.net/assets/downloads/global-ocindex-report.pdf

Euromed Police VI
The main stakeholders and beneficiaries of this component are law enforcement agencies (including police, gendarmerie, immigration services, customs, border guards and other services with tasks relating to the prevention and fight against serious organised crime, terrorism and other crimes), as well as public ministries, central authorities, and legislative and judicial institutions, taking a holistic approach in encouraging cooperation of all relevant security agencies in partner countries.

Component 2: CyberSouth+
Key stakeholders for criminal justice action on cybercrime and other offences involving electronic evidence are ministry of justice, ministry of interior, ministry of technologies and communication, ministry of defence, judiciary, police, national training institution, CERTs, CSIRTs, National Cybersecurity Agency, Authority on Data Protection, national and international service providers, academia.

2.3. Lessons Learned

Euromed Police VI:

The fifth phase of Euromed Police marked the transfer of the project to CEPOL and Europol, which represented a new step towards an EU coordinated approach for the South Partner Countries. Having the programme directly implemented by EU Justice and Home Affairs agencies is a key element to strengthen the strategic and operational police cooperation between SPCs and the EU. Euromed Police can indeed offer a platform for dialogue and exchange, which may then lead to other types of arrangements/cooperation. The first working arrangement between Tunisia and CEPOL signed in March 2022 is a good example.

Although the project started in the online environment, due to travel restrictions, the Agencies succeeded in developing the law enforcement community. The delivery of the Operational Training Need Analysis represented an important milestone in transferring the methodology to the project partners, based on EMPACT crime priorities.

The project took a proactive approach and successfully integrated the EMPACT community in the delivery of the activities (training activities on crime priorities and strategic cooperation forums), which represents a first step towards a coordinated operational approach in the fight against organised crime. In addition, the project proposed for the first time Operational Actions on capacity building activities under the Common Horizontal Strategic Goal 8 (OAPs 2023 on cyber-attacks, trafficking of drugs, migrant smuggling, illicit trafficking of firearms), which will further expand the external dimension of EMPACT and the cooperation with partners to address the common challenges in the field of organised crime.

The drafting of the Euromed Threat Assessment (EMTA) contributed to strengthening the culture of continuous data collection and analysis for the process of informing decision makers on current and emerging trends in serious crime landscapes.

The partnership between CEPOL and Europol in the development of the activities appeared to be paramount to mirror the existing cooperation mechanisms at EU level and to enhance the participation of the South Partner Countries partners in EMPACT.

The next phase of Euromed Police will build upon the achievements of phase V. It will contribute to further expand the external dimension of the EMPACT-cycle in the Southern Neighbourhood region to address the common challenges of organised crime. The project will develop the concept of an EMPACT support network, to foster the multidisciplinary approach towards the fight against organised crime. It will also

further promote regional coordination by integrating Southern Partner Countries within the analysts' community through Europol's Platform for Experts.

CyberSouth+:

The EU has been actively financing several actions aimed to address issues related to the fight against cybercrime in the Southern Neighbourhood. CyberSouth+ will build on lessons learned from the first phase of CyberSouth, which has been supporting Algeria, Jordan, Lebanon, Morocco and Tunisia since 2017. It will continue to support the reform of domestic legislation in line with the Budapest Convention on Cybercrime. The support will however be extended to the alignment with the Second Additional Protocol on electronic evidence. As mentioned previously, only Morocco is a Party to the Convention.

The project will also continue building the capacity of the judiciary to effectively investigate and prosecute cybercrime. Algeria has integrated basic and advanced trainings on cybercrime in the curriculum of its judicial training institute. Tunisia and Jordan have basic trainings in place but revision of the material might be needed. Lebanon and Morocco still need to integrate the new curricula. The second phase of CyberSouth will focus on more advanced training and on "Train the Trainers" courses to ensure the sustainability of the support provided.

The project will also integrate a novelty and contribute to greater synergies between criminal justice and cybersecurity responses to cyber threats, by supporting mechanisms for trusted cooperation and reporting between cybersecurity institutions and criminal justice authorities. Finally, the geographical scope of the project will be extended to cover the entire Southern Neighbourhood region, including Egypt, Libya and Palestine*.

CyberSouth+ will also build upon the achievements of other regional projects and will continue working in close collaborations with them. For instance, the regional programme "Euromed Police V" and "Euromed Justice V" have had cybercrime high on the agenda, addressing respectively capacity-building of police officers and prosecutors/judges in South Partner Countries. Under the programme "Euromed Justice V", a network of practitioners has been established on cybercrime and digital evidence. This sub-group is meant to liaise with the European Judicial Network in order to ease to cooperation between South Partner Countries and EU Member States. CyberSouth+ will also work in close cooperation with the programme South V implemented by the Council of Europe and which works, among other things, on the alignment with the Convention 108+.

Finally, this component will also capitalise on the lessons identified and the experience gained through ongoing bilateral projects, such as the project "Advance Counter Terrorism for Lebanon security", which aims to improve cyber-security and protection and response against cyber-terrorism.

3. DESCRIPTION OF THE ACTION

3.1. Objectives and Expected Outputs

The **Overall Objective (Impact)** of this action is to make the Southern Neighbourhood safer, more secured, and better equipped to fight organised crime and related cyber threats.

The **Specific Objective(s) (Outcomes)** of this action are:

1. The strategic and operational capacities of Southern Partner Countries (SPCs) to protect their citizens against transnational serious and organised crime are enhanced **(component 1).**

2. The criminal justice capacities for enhanced cooperation on cybercrime and disclosure of electronic evidence in the Southern Neighbourhood are strengthened in line with human rights and rule of law, **(component 2).**

The **Outputs** to be delivered by this action contributing to the corresponding Specific Objectives (Outcomes) are:

1.1 contributing to **Specific Objective 1 (or Outcome 1)**: The evidence-based identification of priority crime areas in the Southern Neighbourhood is enhanced.

1.2 contributing to **Specific Objective 1 (or Outcome 1)**: The capacities of SPCs to provide a sustainable law enforcement training system, capable to cater for the actual needs of law enforcement professionals on the one hand, and able to self-diagnose training needs and re-cascade training achievements on the other hand, are enhanced.

1.3 contributing to **Specific Objective 1 (or Outcome 1)**: The strategic cooperation between national law enforcement authorities in SPCs, as well as between SPCs and EU MS and EU agencies, is enhanced.

1.4 contributing to **Specific Objective 2 (or Outcome 2)**: The compliance of domestic legislation on cybercrime and electronic evidence with the Budapest Convention and its Second Protocol is enhanced.

1.5 contributing to **Specific Objective 2 (or Outcome 2**): The capacity of criminal justice authorities to prosecute cybercrime and cases involving e-evidence is enhanced.

1.6 contributing to **Specific Objective 2 (or Outcome 2)**: The capacity of criminal justice authorities to engage in international and public/private cooperation using the tools of the Convention and its Second Protocol is enhanced.

1.7 contributing **Specific Objective 2 (or Outcome 2)**: The synergies between criminal justice and cybersecurity responses to cyber threats are reinforced.

3.2. Indicative Activities

<u>Component 1: Euromed Police VI</u>

The main indicative activities are:

For Result 1:

- Update of the EUROMED Threat Assessment (EMTA) to identify and specify the most threatening criminal phenomena in the MENA Region. The project will seek to increase the independence of the Analysis Single Points of Contacts (ANASPOCs) in drafting the EMTA, based on the knowledge they have built up during EUROMED V.

For Result 2:

- Operational Training Needs Analysis for 2024-2028
- Joint residential training on thematic areas for law enforcement specialists from partner countries and EU Member States organised in SPC on identified training needs corresponding to EU crime priorities.
- Euromed Mobility Scheme implemented via CEPOL's flagship Exchange Programme (CEP).

- Tabletop and real size exercises in close cooperation with any specific operational action in relevant OAPs.
- Fostering E-learning and blended learning via CEPOL Learning Platform.
- Development of the multiplication training courses and a pool of national trainers to ensure cascading sessions.
- Yearly workshops on strategic analysis and review of the key stages in the analytical process (terms of reference, data collection plan, report).

For Result 3:

- Annual Strategic Cooperation Forums to enable the exchange of information and good practices and ensure the identification of the strategic needs (validation of the Operational Training Needs Analysis (OTNA) and the training solutions). These meetings could also offer the opportunity for informal bilateral meetings on real operational cases, in particular between SPC and EU MS.
- Development of the concept of the EMPACT support network, to foster the multidisciplinary approach and to develop guidelines and methodologies on the risk profiles identified. The network will be developed by mirroring the EMPACT priorities with the crime areas identified in the SPC and the activities will be thematic driven.
- Integration of the regional network of analysis single points of contact (ANASPOC) within the Europol's Platform for Experts (EPE), specifically the platform on criminal analysis (CONAN).

<u>Component 2: CyberSouth+</u>

The main indicative activities are:

For Result 1:

- Carry out a comprehensive assessment of domestic legislation regulating cybercrime and electronic evidence.
- Provide legal expertise to reform applicable laws and regulations implementing the provisions of the Budapest Convention.
- Provide technical expertise to review and update national cybersecurity strategies or action plans in terms of their coverage of the criminal justice response.
-

For Result 2:

- Support policy dialogue and organise workshops with training institutions to review training strategies and curricula.
- (Re-)train the trainers of domestic training institutions.
- Integrate in and deliver basic, intermediate and advanced cybercrime/e-evidence training programmes for prosecutors and judges through domestic training institutions.
- Deliver and/or support advanced training on specialised topics regarding cybercrime investigations, virtual currency investigations and digital forensics.
- Facilitate the delivery of cybercrime/e-evidence training to defence attorneys with the use of the HELP training courses in national languages.
- Organise cybercrime exercises focusing on the tools of the Second Additional Protocol.
- Deliver case simulation exercises on cybercrime investigations and digital forensics for relevant agencies/entities in cooperation with other C-PROC projects.
- In cooperation with the programme South V, raise awareness and promote alignment with the Convention 108+ for the protection of individuals with regard to automatic processing of personal data.

For Result 3:

- Government-to-government cooperation: Practical guides, procedures and templates, and domestic and regional training on articles 8 (giving effect to production orders), 9 (expedited disclosure in emergencies), 10 (emergency mutual assistance), 11 (video conferencing) and 12 (joint investigation teams and joint investigations) of the Second Protocol. Public/private cooperation: Practical guides, procedures and templates, and domestic and regional training for competent authorities, service provides and registrars on the application of articles 6 (requests for domain name registration information) and 7 (production orders for subscriber information) of the Second Protocol.
- Continued support to participation and networking in INTERPOL/EUROPOL/EUROJUST conferences, T-CY/Octopus, UN and other relevant events.

For Result 4:

- Contribution to the development or update of cybercrime and/or cybersecurity strategies or action plans and review of their effectiveness in terms of cooperation between criminal justice and cybersecurity institutions.
- Development of tools on national cooperation and operative procedures for criminal justice authorities and cybersecurity organisations.
- Development of guides on national cooperation principles and operative procedures for criminal justice authorities and cybersecurity organisations.
- Regional Cybercrime Cooperation Exercises for law enforcement, prosecutors, forensic experts, CSIRTs and specialised investigators involving real-time competitive simulation exercises on cybercrime and cybersecurity.

3.3. Mainstreaming

Environmental Protection, Climate Change and Biodiversity

Not targeted.

Gender equality and empowerment of women and girls

The two components will ensure the equal participation of women and integrate gender perspectives into their activities as a cross-cutting priority and will strive to promote gender equality and equal opportunities. Gender equality incentives will be incorporated particularly in capacity building activities. . Furthermore, the three components will work with partners to ensure a balanced representation of women and men among action beneficiaries to the greatest extent possible (e.g. the action will not propose or accept single-gender workshops, panels, etc.).

As per OECD Gender DAC codes identified in section 1.1, the three components are labelled as G1.

Human Rights

All activities under the two components will be designed and implemented in accordance with the principles of good governance and human rights, gender equality, the inclusion of socially or economically deprived groups and environmental sustainability, wherever these issues are of particular relevance to the institutions and beneficiaries to be assisted. The fight against organised crime also in relation to capacity building, involve a wide range of stakeholders including from security and law enforcement agencies. Therefore, particular focus should be placed in the incorporation of safeguards in the proposed action in relation to

human rights, data protection and good governance, in line with the EU Strategic Framework and Action Plan on Human Rights and Democracy.

Disability

As per OECD Disability DAC codes identified in section 1.1, this action is labelled as D0. This implies that this action and its component are not considered relevant for the inclusion of persons with disabilities.

Democracy

Not a significant objective.

Conflict sensitivity, peace and resilience

The three components of this action aim to contribute to the achievement of SDG 16 (Peace, Security and Strong Institutions), in particular the following targets: 16.3 *Promote the rule of law at the national and international levels and ensure equal access to justice for all*; 16.4. *By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organised crime*; 16.A *Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime*.

Disaster Risk Reduction

Not a significant objective.

3.4. Risks and Assumptions

Category	Risks	Likelihood (High/ Medium/ Low)	Impact (High/ Medium/ Low)	Mitigating measures
Category 1 – Risks related to the external environment	Risk of political tensions between partner countries	**M/H**	**L**	Partner countries can choose between different schemes of co-operation, and actions do not necessarily concern all countries.
Category 1 – Risks related to the external environment	Political instability within some of the partner countries	**H**	**L**	Non-inclusion of countries in crisis will not hamper project implementation.
Category 1 – Risks related to the external environment	Lack of commitment for project implementation	**M**	**L/M**	Partner countries can choose between different levels of partnerships and participation is on a voluntary basis.

Category 1 – Risks related to the external environment	New outbreak of a pandemic crise	**H**	**M/L**	Virtual or hybrid meetings and conferences can replace face-to-face meetings/ missions. The situation will have to be regularly assessed and the work plan adapted if needed.
Category 3 – Risks related to people and the organisation	Lack of trust and limited cooperation among countries	**H**	**M**	The cooperation between participating countries could be promoted in a gradual manner and around consensual matters through a phased approach with clear deliverables and milestones to ensure results and sustainability.
Category 3 – Risks related to people and the organisation	High turnover of staff in the partner countries	**H**	**M**	When possible, each action should include a "train the train" approach at national level in order to ensure the sustainability of the project.

3.5. Intervention Logic

As concerns **Outcome 1**:

Organised criminal groups are increasingly active across criminal markets and ready to adapt their methods to circumstances, highlighting the need for law enforcement response to be agile, swift and coordinated. Serious and organised crime is also becoming more and more trans-regional, representing a shared challenge for both shores of the Mediterranean. Strengthening strategic and operational police cooperation within the Southern Partner Countries and also with the EU is essential to fight effectively transnational organised crime. Tackling serious and organised crime requires that regional cooperation mechanisms be strengthened, starting from a shared threat assessment based on joint analysis.

According to the underlying intervention logic for this action, the following correlations hold true:

IF the law enforcement authorities of Southern Partner Countries are trained to conduct security threats analysis, THEN the support provided will contribute to strengthening the culture of continuous data collection and analysis for the process of informing decision makers on current and emerging trends in serious crime landscapes.

IF the law enforcement authorities of Southern Partner Countries are able to analyse security threats, THEN they will be able to identify priorities crime areas at national and regional levels. The priority crime areas could then constitute a common ground on which to base cross-border, regional cooperation.

IF the law enforcement authorities of Southern Partner Countries have identified the main security threats, THEN they should be able - with the assistance of CEPOL - to identify their needs to combat these threats. To achieve this output, CEPOL will coordinate the Operational Training Needs Analysis, transfer the methodology used at the EU level within the framework of the EMPACT cycle and equip SPCs with the necessary knowledge to conduct it at regional level. CEPOL will also support SPCs with a multiannual, multidisciplinary and multi-layered interactive training portfolio focusing on the identified crime priorities. To ensure the sustainability of the training portfolio, the project will support the development of pool of national trainers to ensure cascading sessions and the multiplication of training courses. These activities

should enhance the capacities of SPCS to provide a sustainable law enforcement training system, capable to cater for the actual needs of law enforcement professionals on the one hand, and able to self-diagnose training needs and re-cascade training achievements on the other hand.

IF the high-level regional dialogue between law enforcement agencies in SPCs continues to be reinforced AND IF the structured collaborative environment between the EU Member States, Justice and Home Affairs Agencies and the MENA countries continues to be consolidated thanks to the EMPACT Support Network, THEN the strategic cooperation between national law enforcement authorities in SPCs, as well as between SPCs and EU Member States and EU agencies will be enhanced. This cooperation could further expand the external dimension of EMPACT and contribute to a coordinated operational approach between SPCs and the EU in the fight against organised crime. It could also ease the participation of SPCs in EMPACT operational action plans (OAPs), when and where relevant and mutually beneficial. The project could also be used as a vector to facilitate the negotiations of working arrangements between CEPOL and Europol and some SPCs, as well as of international agreements between the EU and some SPCs on the exchange of personal data with Europol.

Finally, IF the three project outputs are successfully delivered, the strategic and operational capacities of Southern Partner Countries (SPCs) to protect their citizens against transnational serious and organised crime will be enhanced.

As concerns **Outcome 2**:

Crimes committed online have increased. They represent security threats, which cannot by fought by a single country alone as they often have a trans-national nature.

To investigate and prosecute cybercrime effectively, law enforcement and justice authorities need to cooperate across borders. As they are increasingly dependent on electronic evidence located outside of their jurisdiction, making it easier and quicker to obtain this evidence, while complying with human right standards is also of crucial importance.

According to the underlying intervention logic for this action, the following correlations hold true:

IF based on a comprehensive assessment of domestic legislation, SPCs are willing to receive legal expertise to reform applicable laws and regulations related to cybercrime and electronic evidence and if they are willing to receive technical advice to review and update national cybersecurity strategies or action plans in terms of their coverage of the criminal justice response, then the compliance of domestic legislation on cybercrime and electronic evidence with the Budapest Convention and its Second Protocol will increase.

IF judicial academies receive support to adopt/upgrade their curricula on cybercrime and electronic evidence and if prosecutors, judges and other relevant practitioners receive the appropriate training according to their needs (basic, intermediate and advanced), then the capacity of criminal justice authorities to prosecute cybercrime and cases involving e-evidence will be enhanced. This capacity should tend to be sustainable in the long-term thanks to the training of the trainers of domestic training institutions. IF national authorities are trained on the provisions and requirements of the Budapest Convention concerning government-to-government cooperation (e.g. giving effect to production orders, emergency mutual assistance, joint investigations, etc.) AND public/private cooperation (e.g. requests for domain name registration information, production orders for subscriber information, etc.), THEN the capacity of criminal justice authorities to engage in international and public/private cooperation using the tools of the Convention and its Second Protocol should be enhanced.

IF national authorities in the Southern Neighbourhood receive assistance to review and update their cybercrime and/or cybersecurity strategies or actions plan to ensure the effectiveness of the cooperation between criminal justice and cybersecurity institutions and if tools are made available to facilitate national cooperation and operative procedures between justice authorities and cybersecurity organisations, THEN the synergies between criminal justice and cybersecurity responses to cyber threats should be reinforced.

Finally, if the four project outputs are successfully delivered, the criminal justice capacities for enhanced cooperation on cybercrime and disclosure of electronic evidence in the Southern Neighbourhood will be strengthened in line with human rights and rule of law, including data protection requirements.

3.6. Indicative Logical Framework Matrix

Results	Results chain: Main expected results	Indicators	Baselines (2023)	Targets (2027)	Sources of data	Assumptions
Impact 1	**to make the Southern Neighbourhood safer, more secured, and better equipped to fight organised crime and related cyber threats.**	GO.1.1 Target 16.1 Significantly reduce all forms of violence and related death rates everywhere; Indicator 16.1.4: proportion of population that feel safe walking alone around the area they live GO.1.2. Number of state institutions and non-state actors supported by the EU on security, border management, countering violent extremism, conflict prevention, protection of civilian population and human rights (GERF 2.23)	SDG web-page: Progress of Goals 16 in 2023	SDG web-page Progress of Goals 16 and in 2027	SDG Reviews Progress Reports	*Not applicable*

Outcome 1	The strategic and operational capacities of Southern Partner Countries (SPCs) to protect their citizens against transnational serious and organised crime are enhanced	SO.1.1. Improvement of country's position in in the Organised Crime Index SO.1.2. Number of MoUs, working arrangements between South Partner Countries but also with EU agencies and/or EU Members States, facilitated by the Programme	SO.1.1. Ranking of 2021: Algeria on 104, Egypt on 79th, Israel on 124th, Jordan on 106th , Lebanon on 15th, Libya on 20th, Morocco on 103th, Palestine (no data), Tunisia on 124th SO.1.2. To be assessed during the inception phase (Tunisia has signed working arrangements with CEPOL)	SO.1.1. Improvement by 1 position in the ranking SO.1.2. To be assessed during the inception period.		Governments are committed towards the objectives of the action The security context does not interfere with the implementation of activities. Complex heterogeneity of partner countries with different development and security challenges, languages and levels of institutional capacity does not impede implementation of activities. EU political dialogue is progressing in the EU Neighbourhood South The negotiations on institutionalised cooperation between the MENA partner countries and the Commission on cooperation with Europol are progressing EU MS and JHA agencies support the project implementation International cooperation instruments are evolving in the MENA region

Outcome 2	The criminal justice capacities for enhanced cooperation on cybercrime and disclosure of electronic evidence in the Southern Neighbourhood are strengthened in line with human rights and rule of law, including data protection requirements	SO2.1. Level of investigations, prosecutions, adjudication and international cooperation on cybercrime and electronic evidence	SO2.1. Limited investigations, prosecutions, adjudication and international cooperation on cybercrime and electronic evidence	SO2.1. Measurable qualitative and quantitative increase in investigations, prosecutions, adjudication and international cooperation on cybercrime and electronic evidence	Official law journals CoE Country Wiki T-CY reports Assessments and progress reports carried out by the project National criminal justice annual reports and statistics	Political decisions to request accession or to accede to or ratify the BC and its Second Protocol National cybercrime or cybersecurity strategies are adopted and/or updated by governments based on the recommendations made Criminal justice practitioners will be able to apply the skills acquired on the basis of domestic legislation
		S02.2. Increased availability and quality of legislation on cybercrime and electronic evidence in line with the Budapest Convention (1. number of states that have legislation in line with the Budapest Convention, 2. number of states that have been invited to accede the Budapest Convention)	SO2.2.1: 2 States have legislation compliant with the Budapest Convention, 1 with the First Protocol and 0 with the Second Protocol	SO2.2.1: An additional 2 States will have legislation on cybercrime and e-evidence in line with the Budapest Convention and its Second Protocol		
			SO2.2.2: 1 State invited to accede. 1 Party to the Budapest Convention and its First Protocol as well as signatory to the Second Protocol	SO2.2.2: An additional 2 States will have been invited to accede to the Budapest Convention on Cybercrime, and 1 State will be Party to the Second Protocol		

Outputs						
Output 1 to outcome 1	The evidence-based identification of priority crime areas in the Southern Neighbourhood is enhanced.	Updated Euromed Threat Assessment (EMTA) Increased independence of the ANASPOCs to draft the EMTA [scale: 0.base-line (As it is), 1: slightly enhanced; 2: significantly enhanced 3: capacity adequate to requirements]	0 0	1 2	Project Reports CEPOL web and CEPOL's electronic platform LEEd Europol web	Availability of required officials for training activities Willingness to exchange information and experience with non-national on a peer-to-peer basis Compliance with rule of law, human rights, data protection and privacy principles in (intelligence and) criminal procedures is observed Governments are committed towards the objectives of the action
Output 2 to outcome 1	The capacities of SPCs to provide a sustainable law enforcement training system, capable to cater for the actual needs of law enforcement professionals on the one hand, and able to self-diagnose training needs and re-cascade training achievements on the other hand are enhanced.	Operational Training Needs Analysis for 2024-2028 Number of law enforcement officers trained (women and men) Increased institutional knowledge and capacity on the EMPACT Incorporation of course curricula developed by the project into national training	0 0 limited 1	1 regional, 9 national 800 Increase by 30% 4		

Output 3 to outcome 1	The strategic cooperation between national law enforcement authorities in SPCs, as well as between SPCs and EU MS and EU agencies is enhanced.	Development of the EMPACT support Network Integration of the regional network of ANASPOCs with the Europol's Platform for Experts, especially the platform on criminal analysis (CONAN) Extended to which coordination between SPCs and with EU is enhanced [scale: 0. Base-line, 1: slightly enhanced; 2: significantly enhanced; 3: adequate to requirements]	0 X 0	EMPACT support network in place X + 10% 2		
Output 1 to outcome 2	The compliance of domestic legislation on cybercrime and electronic evidence with the Budapest Convention and its Second Protocol is enhanced.	Draft legislative amendments on cybercrime and e-evidence are 0. Drafted 1. Proposed 2. Discussed and 3, adopted Extent to which national cybersecurity strategies or action plans address the criminal justice response and are aligned with the international standards of the Budapest Convention	Baselines to be determined by the Council of Europe	Targets to be determined by the Council of Europe.	Project (assessment) reports.	Parliaments are ready to discuss and adopt new legislation on cybercrime and e-evidence National cybercrime or cybersecurity strategies are adopted and/or updated by governments based on the recommendations made Criminal justice

Output 2 to outcome 2	The capacity of criminal justice authorities to prosecuting cybercrime and cases involving e-evidence is enhanced	Number of people have acquired the appropriate skills (disaggregated: professional profile, theme of capacity development, gender)	Baselines to be determined by the Council of Europe	Targets to be determined by the Council of Europe	Project (assessment) reports.	practitioners will be able to apply the skills acquired on the basis of domestic legislation Political will to increase international cooperation based on the provisions of the Budapest Convention and its Protocols National criminal legislation includes provisions on international cooperation and MLA The assessment of cybersecurity strategies or action plans will result in their revision Criminal justice and cybersecurity institutions will continue to cooperate on the basis of the SOPs and other tools
Output 3 to outcome 2	The capacity of criminal justice authorities to engage in international and public/private cooperation using the tools of the Convention and its Second Protocol is enhanced	Availability of guides, procedures or templates for requests/responses related to transnational cases Number of assistance requests handled by judicial and police international cooperation department, including with the private sector 24/7 mechanisms in place	No specific guides, procedures or templates for assistance requests in all countries/area Baseline to be determined during the inception period. Limited use of the 24/7 points of contact and other police/judicial cooperation channels available in all countries/area	Procedures and templates for international cooperation are in place in 4 countries Increased number of processed requests (+20%) in 6 countries 24/7 mechanisms in place and functioning	International cooperation departments reports and statistics National reports and statistics on criminal justice Project reports	

Output 4 to outcome 2	The synergies between criminal justice and cybersecurity responses to cyber threats are reinforced.	Revision of National strategies on cybersecurity in line with international standards 0.drafted 1.proposed 3.discussed and 4. Adopted with the assistance of the project Standard operating procedures for cooperation between CERT/CSIRT and criminal justice institutions available	Lack of national strategies on cybersecurity in 4 countries Lack or partial standard operating procedures for national co-ordination in 6 countries Limited data sharing between CSIRTs/CERTs and criminal justice institutions in 8 countries	National strategies on cybersecurity provide for cooperation between CERT/CSIRT and criminal justice institutions in 6 countries Standard Operating Procedures for CERT/CSIRT and criminal justice cooperation available or under development in 4 countries Increased number of cases (+20%) for which cooperation between CERT/CSIRT and criminal justice institutions took place in 6 countries	CERT/CSIRT reports. Project reports on LEA – CERT/CSIRT cooperation Evaluations on national strategies and action plans on cybersecurity	

4. IMPLEMENTATION ARRANGEMENTS

4.1. Financing Agreement

In order to implement this action, it is not envisaged to conclude a financing agreement with the partner countries.

4.2. Indicative Implementation Period

The indicative operational implementation period of this action, during which the activities described in section 3 will be carried out and the corresponding contracts and agreements implemented, is 72 months from the date of adoption by the Commission of this financing Decision.

Extensions of the implementation period may be agreed by the Commission's responsible authorising officer in duly justified cases.

4.3. Implementation Modalities

The Commission will ensure that the EU appropriate rules and procedures for providing financing to third parties are respected, including review procedures, where appropriate, and compliance of the action with EU restrictive measures.[12]

4.3.1. Indirect Management with pillar-assessed entities

A part of this action **(component 1**) may be implemented in indirect management with the European Union Agency for Law Enforcement Training (CEPOL). This implementation entails the objectives and activities described under sections 3.1 and 3.2 (component 1). The envisaged entity has been selected using the following criteria:

- Successful implementation of previous phases of the programme.
- Necessary expertise to implement the objectives and activities.
- Good project experience in the same areas of work in other regions (Eastern Neighbourhood and Western Balkans).
- Possibility of an increased partnership with all EU Member States.

A part of this action **(component 2)** may be implemented in indirect management with the Council of Europe. This implementation entails the objectives and activities described under sections 3.1 and 3.2 (component 2).

The envisaged entity has been selected using the following criteria:

- Successful implementation of previous phases of the programme.
- Necessary expertise to implement the objectives and activities.
- Good project experience in the same areas of work in other regions (Eastern Neighbourhood and Western Balkans).
- Capacity to undertake such initiative
- Solid network of partners in the Southern Neighbourhood.

[12] EU Sanctions Map. Please note that the sanctions map is an IT tool for identifying the sanctions regimes. The source of the sanctions stems from legal acts published in the Official Journal (OJ). In case of discrepancy between the published legal acts and the updates on the website it is the OJ version that prevails.

In case the envisaged entities would need to be replaced, this action may be implemented in indirect management with another pillar-assessed international organisation or with Member States' organisations and consortia thereof. The entrusted entities will be selected after negotiations resulting from a call for manifestation of interest addressed to relevant international organisations and Member States organisations eligible for indirect management.

4.4. Indicative Budget

Indicative Budget components	**EU contribution (amount in EUR)**	**Third-party contribution (amount in EUR)**
Implementation modalities – cf. section 4.3		
Component 1 (Euromed Police VI)		
Indirect management with CEPOL – cf. section 4.3.1	6 000 000	N.A.
Component 2 (CyberSouth+)		
Indirect management with the Council of Europe – cf. section 4.3.1	3 500 000	350 000
Evaluation – cf. section 5.2 **Audit** – cf. section 5.3	will be covered by another Decision	N.A.
Strategic communication and Public diplomacy – cf. section 6	will be covered by another Decision	N.A.
Contingencies	N.A.	N.A.
Totals	**9 500 000**	**350 000**

4.5. Organisational Set-up and Responsibilities

Euromed Police VI: This programme will be directly implemented by CEPOL, in partnership with Europol. The European Commission will supervise the agreement in close liaison with the EU Delegations in the ENP South Partner Countries. A Steering Committee will be established with the participation of the relevant Commission services, especially the Directorate-General Migration and Home Affairs, to which CEPOL reports.

CyberSouth+: This programme will be directly implemented by the Council of Europe. The European Commission will supervise the agreement in close liaison with the EU Delegations in the ENP South Partner Countries. A Steering Committee will be established with the participation of the relevant Commission services and EEAS, especially the Directorate-General Migration and Home Affairs.

5. PERFORMANCE MEASUREMENT

5.1. Monitoring and Reporting

The day-to-day technical and financial monitoring of the implementation of this action will be a continuous process, and part of the implementing partners' responsibilities. To this aim, each implementing partner shall establish a permanent internal, technical and financial monitoring system for the action and elaborate regular progress reports (not less than annual) and final reports. Every report shall provide an accurate account of implementation of the action, difficulties encountered, changes introduced, as well as the degree of achievement of its Outputs and contribution to the achievement of its Outcomes, and if possible at the

time of reporting, contribution to the achievement of its Impacts, as measured by corresponding indicators, using as reference the logframe matrix.

The Commission may undertake additional project monitoring visits both through its own staff and through independent consultants recruited directly by the Commission for independent monitoring reviews (or recruited by the responsible agent contracted by the Commission for implementing such reviews).

Arrangements for monitoring and reporting, including roles and responsibilities for data collection, analysis and monitoring:

The monitoring level will be for each component of the action.

Every component will have its own logical framework, which will be completed during the inception period and updated during implementation.

SDGs indicators and EU Result Framework Indicators should be taken into account.

To ensure a closer follow-up, every implementing partner will provide a monthly Flash Report indicating the past activities, activities in the pipelines, difficulties encountered and measures taken to mitigate.

5.2. Evaluation

Having regard to the nature of the action, a mid-term evaluation will be carried out for this action or its components via independent consultants contracted by the Commission.

It will be carried out for accountability and learning purposes at various levels (including for policy revision), taking into account in particular the complexity and the various topics covered by the action.
The Commission shall form a Reference Group (RG) composed by representatives from the main stakeholders at both EU and national (representatives from the government, from civil society organisations (private sector, NGOs, etc.), etc.) levels. If deemed necessary, other donors will be invited to join.

The Commission shall inform the implementing partners at least 2 months in advance of the dates envisaged for the evaluation exercise and missions. The implementing partners shall collaborate efficiently and effectively with the evaluation experts, and inter alia provide them with all necessary information and documentation, as well as access to the project premises and activities.

The evaluation reports shall be shared with the partner countries and other key stakeholders following the best practice of evaluation dissemination[13]. The implementing partners and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, in agreement with the partner countries, jointly decide on the follow-up actions to be taken and any adjustments necessary, including, if indicated, the reorientation of the project.

The financing of the evaluation shall be covered by another measure constituting a financing Decision.

5.3. Audit and Verifications

Without prejudice to the obligations applicable to contracts concluded for the implementation of this action, the Commission may, on the basis of a risk assessment, contract independent audit or verification assignments for one or several contracts or agreements.

[13] See best practice of evaluation dissemination.

6. STRATEGIC COMMUNICATION AND PUBLIC DIPLOMACY

All entities implementing EU-funded external actions have the contractual obligation to inform the relevant audiences of the Union's support for their work by displaying the EU emblem and a short funding statement as appropriate on all communication materials related to the actions concerned. To that end they must comply with the instructions given in the 2022 guidance document *Communicating and raising EU visibility: Guidance for external actions* (or any successor document).

This obligation will apply equally, regardless of whether the actions concerned are implemented by the Commission, the partner countries, service providers, grant beneficiaries or entrusted or delegated entities such as UN agencies, international financial institutions and agencies of EU Member States. In each case, a reference to the relevant contractual obligations must be included in the respective financing agreement, procurement and grant contracts, and contribution agreements.

For the purpose of enhancing the visibility of the EU and its contribution to this action, the Commission may sign or enter into joint declarations or statements, as part of its prerogative of budget implementation and to safeguard the financial interests of the Union. Visibility and communication measures should also promote transparency and accountability on the use of funds. Effectiveness of communication activities on awareness about the action and its objectives as well as on EU funding of the action should be measured.

Implementing partners shall keep the Commission and the EU Delegation/Office fully informed of the planning and implementation of specific visibility and communication activities before the implementation. Implementing partners will ensure adequate visibility of EU financing and will report on visibility and communication actions as well as the results of the overall action to the relevant monitoring committees.

Security issues or local political sensitivities may make it preferable or necessary to limit communication and visibility activities. In such cases, the target audience and the visibility tools, products and channels to be used in promoting a given action will be determined on a case-by-case basis, in consultation and agreement with the European Union.

Appendix 1: IDENTIFICATION OF THE PRIMARY INTERVENTION LEVEL FOR REPORTING IN OPSYS

A primary intervention (project/programme) is a coherent set of results structured in a logical framework aiming at delivering development change or progress. Identifying the level of the primary intervention will allow for:

- ✓ Differentiating these actions or contracts from those that do not produce direct reportable development results, defined as support entities (i.e. audits, evaluations);
- ✓ Articulating actions and/or contracts according to an expected common chain of results and therefore allowing them to ensure a more efficient and aggregated monitoring and reporting of performance;
- ✓ Having a complete and exhaustive mapping of all results-bearing actions and contracts.

The present action identifies as

Action level (i.e. budget support, blending)		
☐	Single action	Present action: all contracts in the present action
Group of actions level (i.e: i) top-up cases, ii) second, third, etc. phases of a programme)		
☐	Group of actions	Actions reference (CRIS#/OPSYS#):
Contract level (i.e. grants, contribution agreements, any case in which foreseen individual legal commitments identified in the budget will have different log frames, even if part of the same action document)		
☒	Single contract 1	Component 1
☒	Single contract 2	Component 2
	(…)	
Group of contracts level (i.e: i) series of programme estimates, ii) cases in which an action document foresees many foreseen individual legal commitments (for instance four contracts and one of them being a technical assistance) and two of them, a technical assistance contract and a contribution agreement, aim at the same objectives and complement each other, iii) follow up contracts that share the same log frame of the original contract)		
☐	Group of contracts	