GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Project Summary

Version 10 February 2022

Project title / number:	GLACY+ (3148) – Global Action on Cybercrime Extended – Joint project of the European Union and the Council of Europe
Project area:	Multiple countries in Africa, Asia/Pacific and Latin America
Duration:	96 months (1 March 2016 – 28 February 2024)
Budget:	EURO 18,890,000
Funding:	Joint project of the European Union (Instrument Contributing to Peace and Stability) and the Council of Europe
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe and INTERPOL

BACKGROUND

The GLACY+ Project (Global Action on Cybercrime Extended), launched in October 2016, is a joint project of the European Union and the Council of Europe, financed by the European Union under the Instrument Contributing to Peace and Stability and implemented by the Council of Europe.

The overall objective of GLACY+ is to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area. Under this overall objective, the Project implements activities worldwide across three specific objectives, that is: (1) Policies and strategies, (2) law enforcement capacities, and (3) criminal justice capacities. The second objective is implemented by INTERPOL through its Global Complex for Innovation, following a strategic partnership agreed between the Council of Europe and INTERPOL.

The Project currently has 17 priority countries (Benin, Brazil, Burkina Faso, Cabo Verde, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Nigeria, Paraguay, Philippines, Senegal, Sri Lanka and Tonga). Some of these countries may be used as hubs to disseminate and multiplicate the effect of the project in their respective regions.

Although the project mainly targets these priority countries, it may also implement activities in other countries, upon request, in particular concerning support to enhance legislative compliance between national legal frameworks and the Budapest Convention on Cybercrime and its additional protocols.

CONTACTS

Catalina STROE	Martha STICKINGS	Virgil SPIRIDON	Alexander SEGER
Project Manager,	Project Manager,	Head of Operations,	Head of Cybercrime
GLACY+	GLACY+	C-PROC	Division, Council of Europe
Catalina.Stroe@coe.int	Martha.Stickings@coe.int	Virgil.Spiridon@coe.int	Alexander.Seger@Coe.Int

www.coe.int/cybercrime

Financé par l'Union européenne et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Mis en œuvre par le Conseil de l'Europe

OBJECTIVE AND EXPECTED RESULTS

Project purpose	**To strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.**
Objective 1	**To promote consistent cybercrime legislation, policies and strategies.**
Result 1.1	Cybercrime policies and strategies are strengthened in up to 20 countries, including relevant aspects of cybersecurity and partnerships with private sector, and experience is shared with further countries.
Result 1.2	Policy dialogue and cooperation on cybercrime enhanced between priority countries and their regions, international and regional organisations, and synergies maximized with EU-funded (notably IcSP-funded) projects developed in project areas.
Result 1.3	Legislation on cybercrime electronic evidence and related data protection provisions are strengthened in line with the Budapest Convention and its Protocols as well as rule of law and human rights standards in priority countries and reforms initiated in additional countries.
Result 1.4	Dialogue between criminal justice practitioners and policymakers and legislators on matters related to legislation and international cooperation on cybercrime and electronic evidence strengthened
Objective 2	**To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions.**
Result 2.1	Assessments/cyber reviews (initial and final) of law enforcement capacities available for priority countries.
Result 2.2	Cybercrime and computer forensics units strengthened in priority countries and experience shared with other countries.
Result 2.3	Law enforcement training strategies available in priority countries, including access to ECTEG training materials
Result 2.4	At least 1000 law enforcement officers trained in basic cybercrime investigations and computer forensics as well as related rule of law requirements
Result 2.5	International police-to-police cooperation on cybercrime and electronic evidence is more effective
Result 2.6	Interagency cooperation strengthened amongst cybercrime units, financial investigators and financial intelligence units in the search, seizure and confiscation of online crime proceeds
Objective 3	**To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation**
Result 3.1	Assessments of criminal justice capabilities available for priority countries
Result 3.2	Judicial training academies in priority countries are providing training on cybercrime and electronic evidence as part of their regular curricula and experience has been shared with other countries
Result 3.3	Institutions strengthened and procedures improved for international judicial cooperation related to cybercrime and electronic evidence in at least 20 countries and experience shared with other countries
Result 3.4	Training centres, academic institutions and other entities providing criminal justice capacity building programs with a regional scope are strengthened and training on cybercrime and electronic evidence is streamlined in the respective curricula
Result 3.5	Criminal justice capacities enhanced on emerging issues related to cybercrime and electronic evidence and their implication for legislation
Result 3.6	Criminal justice response is adapted to address challenges related to the COVID-19 pandemic and its aftermath with respect to news ways of conducting investigation, handling electronic evidence, and conducting remote criminal proceedings

Cybercrime Program Office of the Council of Europe
UN House
48A Primaverii Blvd, 011975 Bucarest, Romania

Tel. : +40 21 201 78 87
E-mail : alexander.seger@coe.int
http://www.coe.int/cybercrime