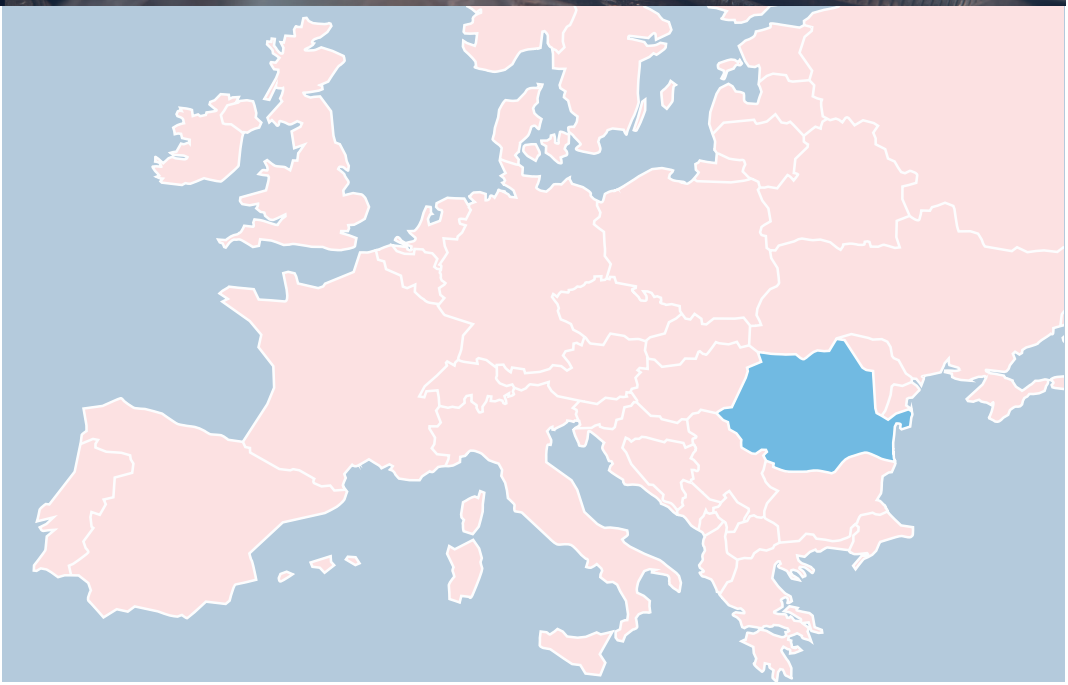
Deutsch-Rumänische
Industrie- und Handelskammer
Camera de Comerț și Industrie
Româno-Germană

*presents:*

# FINANCING INSTRUMENTS AND EU FUNDS

THE BROCHURE



HIGGINS

# HIGGINS

**Founded in Berlin in 2014 as a sales agent and business consultancy, today, HIGGINS is active in over 20 countries around the world. We maintain offices in Berlin, Bucharest and Belgrade and work particularly close with Romania and the countries in Eastern Europe and the West Balkan region.**

**In Bucharest, we have a motivated team of experts in their fields and maintain an office with showroom. Our team and network form an ideal base for companies to build upon while discovering the Romanian market in.**

**In our experience, it is prerogative to know the economic and political landscape when entering a new market, and we are happy to be able to offer this to our partners in Romania, Europe, and worldwide.**

**While we cover the entire range of services for our partners, we have particular expertise in industries like Security&Defense, Cyber Security, IT, and Environment.**

**Together with our strong network, we are doing our best to protect our partners' interests every day and we are proud to count some of the leading players in their respective industries to them.**

**SERVICES**

Business development consultancy;
Market research & Public discussion monitoring;
Public tenders monitoring, planning and support;
International network of partners;
24/7 support of our motivated team in Berlin, Bucharest, Belgrade;
Licenses and concessions;
Cooperation with public entities and companies;
Introduction & representation with state/local authorities.

**CONTACT**

Phone: +40737.55.33.44
E-Mail: mail@higgins.de
Website: www.higgins.de

# Making Use of EU Funds for Security Related Research and Innovation in Romania. Financial instruments and EU funds in the field of Security



Security understood in a wider sense and stretching out to concepts like societal resilience has become a major policy of the European Union in recent years. Last but not least this is reflected in the documents underpinning the Union's Multiannual Financial Framework 2021-27 and its components, among them the Horizon Europe framework programme for research and innovation and the ground-breaking Next-Generation EU-Programme (NGEU) aiming to overcome the consequences of the COVID-19 pandemic.

The Horizon Europe programme offers the greatest number of opportunities for EU funded research. For researchers and enterprises active in the field that are located in Romania, the Romanian part of the NGEU is of particular importance. In 2021, the Government in Bucharest has developed an ambitious programme for the reconstruction of the Romanian economy and society that shall enable the country to meet the challenges of the 21st century – among them many related to security issues.

## I. Horizon Europe

In the framework of the EU research programme 'Horizon Europe' (2020-27) Cluster 3 relates to security, including cybersecurity, and disaster risk reduction and resilience. In addition, it will build on lessons learnt from the COVID-19 crisis in terms of prevention, mitigation, preparedness and capacity building for crises. It is expected that projects develop new knowledge, technologies and/or other solutions related to civil-security issues and are targeted to practitioner needs. Projects will involve practitioner end-users (usually relevant national authorities) alongside researchers and industry.

The cluster is comprised of six funding 'destinations' (meaning general goals that are in line with EU policies ). Each of these 'destinations' is comprised of several calls and research themes (topics). Contrary to many other EU research-programmes, because of the sensitive nature of those areas and the interest to ensure confidentiality and maintain strategic autonomy, co-operation with partners from outside the EU is not encouraged in destinations 1-5. If unavoidable, it is limited to selected international partners only, must be based on reciprocity and contribute to wider strategic goals of the EU.

The Work Programme 2021-22 of Cluster 3 comprises a EU-wide budget of ~ 427.94 mln. €, out of which ~ 195.85 mln. € are earmarked for the 2022 Calls for Proposals (hereinafter: calls):

**1. Destination 1 – Better Protect the EU and its Citizens against Crime and Terrorism.**
Aim: More effective tackling of crime and terrorism while respecting fundamental rights, thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal

and technological aspects, and the development of cutting-edge capabilities for police authorities, including measures against cybercrime.

Proposals under Destination 1 should contribute to:

• Information analysis for police authorities to fight criminals and terrorists using novel technologies efficiently.

• Improved forensics and evidence collection to apprehend criminals and terrorists and bring them to the court.

• Enhanced prevention, detection and deterrence of societal issues related to various forms of crime (cybercrime, terrorism, violent radicalisation, domestic and sexual violence, juvenile offenders, etc.).

• Security against terrorism in public spaces.

•Intelligence picture and prevention, detection and deterrence of organised crime.

• Secure cyberspace for citizens, especially children, through prevention and detection of and protection from cybercriminal activities.

The following calls contribute to this destination:

*- HORIZON-CL3-2022-FCT-01-01:*

Improved crime scene investigations related to transfer, persistence and background abundance

*- HORIZON-CL3-2022-FCT-01-02:*

Better understanding the influence of organisational cultures and human interactions in the forensic context as well as a common lexicon

*- HORIZON-CL3-2022-FCT-01-03:*

Enhanced fight against the abuse of online gaming culture by extremists

*- HORIZON-CL3-2022-FCT-01-04:*

Public spaces are protected while respecting privacy and avoiding mass surveillance

*-HORIZON-CL3-2022-FCT-01-05;HORIZON-CL3-2022-FCT-01-06, and HORIZON-CL3-2022-FCT-01-07:*

Effective fight against trafficking in human beings

**2. Destination 2 – Effective Management of EU External Borders**

Aim: Improved air, land and sea border management and maritime security – including better knowledge on social factors – to facilitate legitimate passengers and shipments travel into the EU while preventing illicit trades, trafficking, piracy, terrorist and other criminal acts.

The following calls contribute to this destination:

*- HORIZON-CL3-2022-BM-01-01:*

Improved underwater detection and control capabilities to protect maritime areas and sea harbours

*- HORIZON-CL3-2022-BM-01-02:*

Enhanced security of, and combating the frauds on, identity management and identity and travel documents

*- HORIZON-CL3-2022-BM-01-03:*

Better, more portable and quicker analysis and detection for customs

*- HORIZON-CL3-2022-BM-01-04:*

Open topic (proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions within this Destination that are not covered by the other topics)

*- HORIZON-CL3-2022-BM-01-05:*

Open topic (proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions within this Destination that are not covered by the other topics)

**3. Destination 3 – Resilient Infrastructure**

Aim: Strengthening the resilience and autonomy of physical and digital infrastructures through more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for infrastructure operators.

The following two calls contribute to this destination:

- *HORIZON-CL3-2022-INFRA-01-01:* Nature-based Solutions integrated to protect local infrastructure
- *HORIZON-CL3-2022-INFRA-01-02:* Autonomous systems used for infrastructure protection

**4. Destination 4 – Increased Cybersecurity**

Aim: Better cybersecurity and a more secure online environment by development and effective use of digital technologies, while respecting fundamental rights. Contribution to the development of robust services, processes, products, and digital infrastructures capable to resist and counter cyber-attacks and hybrid threats.

The following four calls contribute to this destination:

- *HORIZON-CL3-2022-CS-01-01:* Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures
- *HORIZON-CL3-2022-CS-01-02:* Trustworthy methodologies, tools and data security 'by design' for dynamic testing of potentially vulnerable, insecure hardware and software components
- *HORIZON-CL3-2022-CS-01-03:* Transition towards Quantum-Resistant Cryptography
- *HORIZON-CL3-2022-CS-01-04:* Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

**5. Destination 5 – Disaster-Resilient Society for Europe**

Aim: Avoiding losses from natural, accidental and man-made disasters through preventive actions, better societal preparedness, and resilience and improved disaster risk management in a systemic way.

The following nine calls contribute to this destination:

- *HORIZON-CL3-2022-DRS-01-01:* Enhanced citizen preparedness in the event of a disaster or crisis-related emergency
- *HORIZON-CL3-2022-DRS-01-02:* Enhanced preparedness and management of High-Impact Low-Probability or unexpected events
- *HORIZON-CL3-2022-DRS-01-03:* Improved quality assurance / quality control of data used in decision-making related to risk management of natural hazards, accidents and CBRN events
- *HORIZON-CL3-2022-DRS-01-04:* Better understanding of citizens' behavioural and psychological reactions in the event of a disaster or crisis situation
- *HORIZON-CL3-2022-DRS-01-05:* Improved impact forecasting and early warning systems supporting the rapid deployment of first responders in vulnerable areas
- *HORIZON-CL3-2022-DRS-01-06:* Improved disaster risk pricing assessment
- *HORIZON-CL3-2022-DRS-01-07:* Improved international cooperation addressing first responder capability gaps
- *HORIZON-CL3-2022-DRS-01-08:* Enhanced situational awareness and preparedness of first responders and improved capacities to minimise time-to-react in urban areas in the case of CBRN-E-related events
- *HORIZON-CL3-2022-DRS-01-08:* Enhanced capacities of first responders more efficient rescue operations, including decontamination of infrastructures in the case of a CBRN-E event

**6. Destination 6 – SSRI: Strengthened Security Research and Innovation**

Aim: Avoid sector specific bias and blinkers

that impede the proliferation of security solutions, support innovation uptake and go-to-market strategies.

The following four calls contribute to this destination:
- *HORIZON-CL3-2022-SSRI-01-01:*
Increased foresight capacity for security
- *HORIZON-CL3-2022-SSRI-01-02:*
Knowledge networks for security research & innovation
- *HORIZON-CL3-2022-SSRI-01-03:*
Stronger grounds for pre-commercial procurement of innovative security technologies
- *HORIZON-CL3-2022-SSRI-01-04:*
Social innovations as enablers of security solutions and increased security perception

## II. Other relevant EU programmes

**A. Digital Europe Programme (DIGITAL)**

The Digital Europe Programme for cybersecurity capabilities and law enforcement digital capabilities will speed up the take-up of R&I projects in the area of Artificial Intelligence, High Performance computer and cyber security. The programme will also offer infrastructure to the research community.

**B. European Defence Fund (EDF)**

The European Defence Fund (EDF) is the Commission's initiative to support collaborative defence research and development, and to foster an innovative and competitive defence industrial base.
Under the EDF, the EU is providing support all along the lifecycle, from research to prototype development up to certification. Only collaborative projects are eligible. Research actions can receive up to 100% of EU funding of the eligible costs, mainly in grants, while development actions are co-funded. The Fund will complement Member States' investment by co-financing up to 20% of the costs for prototype development and up to 80% of ensuing certification and testing activities.

**C. Integrated Border Management Fund (IBMF)**

The Integrated Border Management Fund (IBMF) is a 2021-27 funding programme made up of two components: the Border Management and Visa Instrument and the Customs Control Equipment Instrument. IBMF aims to support the customs union and customs authorities in their mission to protect the financial and economic interests of the Union and its Member States, to ensure security and safety within the Union and to protect the Union from illegal trade while facilitating legitimate business activity.

**D. Internal Security Fund (ISF)**

The ISF has three objectives
- Increase information exchange among and within the EU law enforcement, and other competent authorities and relevant EU bodies, as well as with non-EU countries, and international organisations;
- Intensify cross-border cooperation, including joint operations, among and within the EU law enforcement and other competent authorities, in relation to terrorism and serious and organised crime with a cross-border dimension;
- Support efforts to strengthen capabilities to combat and prevent crime, terrorism and radicalisation, as well as manage security-related incidents, risks and crises, in particular through increased cooperation between public authorities, civil society and private partners across the Member States.
Beneficiaries of the ISF can be: State/federal police, customs and other specialised law enforcement services (including national cybercrime units, anti-terrorism and

other specialised units), local public bodies, non-governmental organisations, international organisations, Union agencies, private and public law companies, networks and research institutes and universities.

**E. EU Civil Protection Mechanism (EUCPM)**
In addition, synergies can be sought with the Union Civil Protection Mechanism (EUCPM), including via opportunities such as the Union Civil Protection Knowledge Network, Prevention & Preparedness projects, developing additional reserve capacities under rescEU for major and simultaneous disasters, and by co-financing the deployment of Member States' national response capacities.

## III. NextGeneration EU Romania

On September 27, 2021, the European Commission endorsed Romania's 'Recovery and Resilience Plan' (RRP). This was an important step towards the EU disbursing 14.2 bln.€ in grants and 14.9 bln.€ in loans to Romania under the Recovery and Resilience Facility (RRF) to overcome the economic and societal consequences of the COVID-19 pandemic. Divided into 15 'Components', Romania's plan proposes projects in each of the seven EU 'flagship areas' to be addressed by the RRF. A first grant instalment of 1.8 bln. € has been disbursed on December 2nd, 2021.

'Component 7' of the 15 components of the Romanian plan is dedicated to the digital transformation of the country in the 2021-27 period and beyond. The budget of Component 7 is up to 1.5 bln. € until 2027, added by 470 mln. € and 881 mln. € for digitalisation in the healthcare- and education sectors, respectively. Financial contributions are paid in instalments once the Member State has satisfactorily fulfilled the relevant milestones and targets identified in relation to the implementation of the RRP.
Four reform projects and 19 investment-projects related to digitalisation are outlined in Component 7, out of which one reform and four investment-projects explicitly refer to cybersecurity. All of those projects, listed below, are financed from the non-refundable grant share of Romania's RRF-participation:
- Reform 7.3.: Ensuring cybersecurity of public and private entities owning critical value infrastructure
- Investment 7.12: Ensuring cybersecurity protection for both public and private IT & C infrastructures with critical value for national security, using smart technologies
- Investment 7.13: Development of security systems for the protection of the government spectrum
- Investment 7.14: Increase of the resilience and cybersecurity of Internet Service Provider infrastructure services provided to public authorities in Romania
- Investment 7.15: Creation of new cybersecurity skills for society and the economy

An Additional Funding Opportunity under the NGEU Romania
Beyond 'Component 7: Digital Transformation', 'Component 9: Business Support, Research, Research and Innovation' outlines an interesting policy that might be of relevance for enterprises or other legal entities that plan to take part in the Horizon Europe programme:
Investment 7. Strengthening excellence and supporting Romania's participation in partnerships and missions in Horizon Europe aims at increasing the success rates of Romanian applications for Horizon Europe programme.
The investment shall grant complementary

funding to research, development and innovation projects that are already contracted in the context of green or digital European research development and innovation Partnerships.

Measures envisaged are:

• Co-funding research projects recommended for funding under European Partnerships for the transition period (2022-2023) – Horizon Europe (based on the work programme conditions from Horizon Europe). Up to 20 projects shall be financed with a maximum budget of EUR 300 000 for each Romanian partner;

• Complementary projects with the purpose to increase the impact of H2020 projects that are already funded (ongoing or recently finalised). Up to 15 projects shall be financed with a maximum budget of EUR 1 000 000;

• Capacity building projects. Up to 20 projects shall be financed with a maximum budget of EUR 500 000.

The implementation of the investment shall be completed by 31 December 2023, EU support for this reform-project will be disbursed to Romania in the fifth instalment.

**Further information can be provided on request addressed to**
**HIGGINS Cooperation Management GmbH**
**Walter-Benjamin-Platz 4**
**10629 Berlin, Germany**
**www.higgins.de**