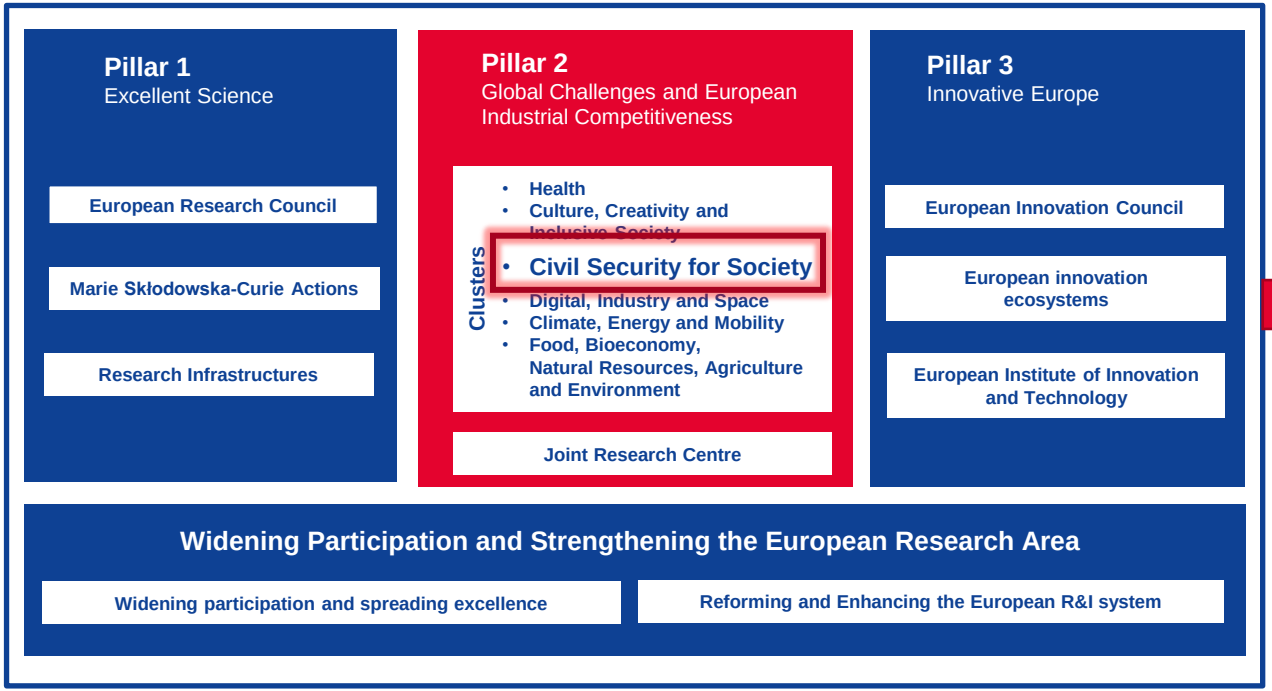
FORSCHUNGSFÖRDERUNG FÜR SOUVERÄNITÄT UND SICHERHEIT IN EUROPA

FFG
Forschung wirkt.

HORIZON EUROPE (2021 – 2027)

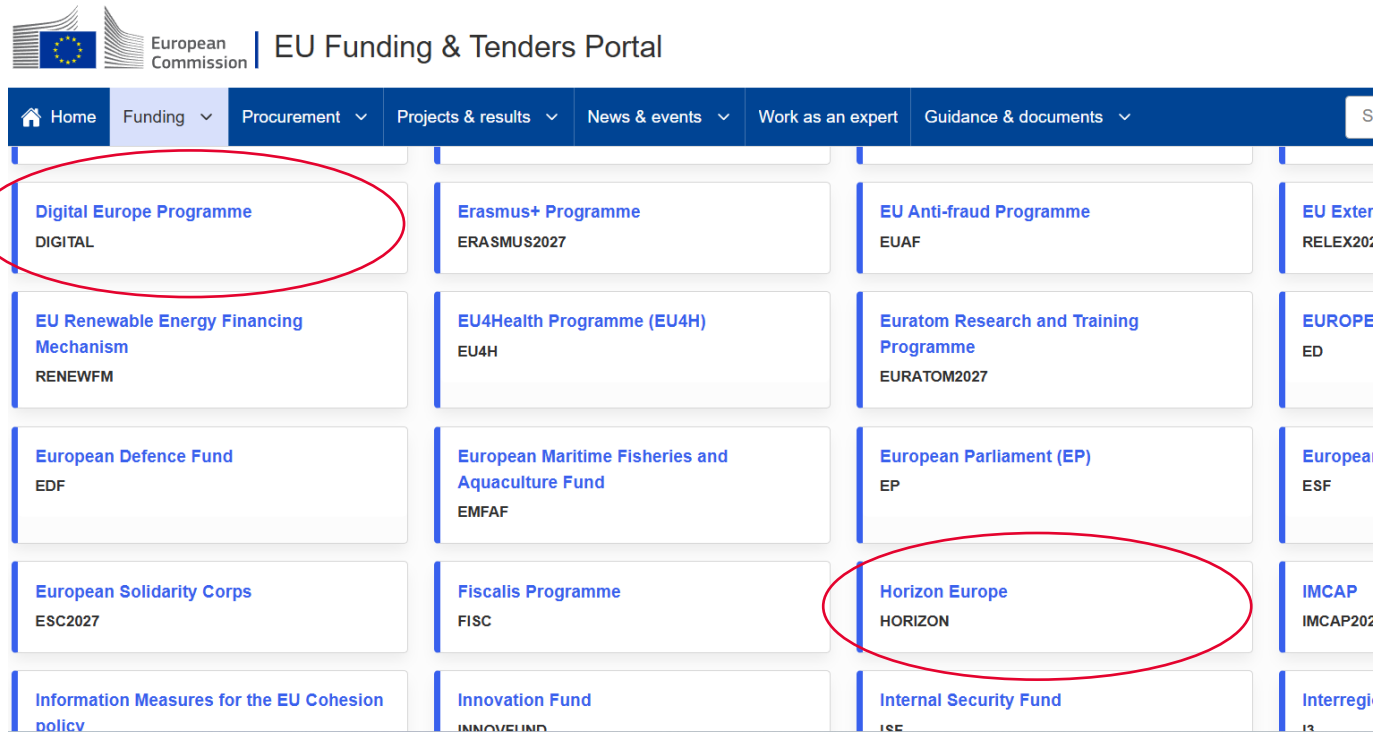
>> ÜBERBLICK – SYNERGIEN



- **European Defence Fund (EDF)**
- **Digital Europe Programme (DIGITAL)**
- **European Cybersecurity Competence Centre (ECCC) + National Coordination Centre**
- Internal Security Fund (ISF)
- Border Management and Visa Instrument (BMVI)
- Customs Control Equipment Instrument (CCEI)
- Union Civil Protection Mechanism (UCPM)
- Austrian Security Research Programme KIRAS/K-PASS/FORTE
- …

EU FUNDING & TENDERS PORTAL

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes



HORIZON EUROPE CLUSTER 3

>>INNOVATIONEN FÜR EUROPAS SICHERHEIT

Entwicklung von Lösungen zur Bewältigung von Krisen, Katastrophen, Kriminalität und anderen Bedrohungen für die Gesellschaft und Infra-strukturen, einschließlich Cyberbedrohungen!

- Gesellschaft und Demokratie stärken;
- den digitalen Wandel sichern;
- die Auswirkungen des Klimawandels mindern;
- rechtmäßige und ethische Ergebnisse gewährleisten;
- die Europäische Wettbewerbsfähigkeit ausbauen;

Die Projektergebnisse sollen für ein breites Spektrum von Endnutzern und Forschenden relevant und anwendbar sein:

- **Forschung & Wissenschaft:** Universitäten, Forschungseinrichtungen
- **Wirtschaft:** KMU, Industrie
- **Öffentliche Hand & Praxis:** Ministerien, Behörden, Einsatzkräfte, Betreiber kritischer Infrastrukturen
- **Zivilgesellschaft:** Bürgerinitiativen, NGOs

Mindestteilnahmebedingungen:

mindestens drei voneinander unabhängigen Rechtsträger aus unterschiedlichen EU Mitgliedsstaaten oder zu HE assoziierten Staaten, davon muss ein Rechtsträger den Sitz in einem EU-Mitgliedstaat haben.

AUSSCHREIBUNGEN 2026/2027

>> PROJEKTARTEN / FÖRDERRATEN

Research and Innovation Actions (RIA)	Innovation Actions (IA)		Coordination and Support Actions (CSA)	Pre-Commercial Procurement (PCP)
100%	100% non profit organisations	70% profit making entities	100%	100%

\+ flat rate of 25% of eligible direct costs

Lump Sum Ansatz für einige Topics!

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/horizon/lump-sum

https://www.ffg.at/europa/heu/recht-finanzen/thema_lumpsum-funding

CL3 – CALLS 2026/2027

>> KURZINFO CALLS CIVIL SECURITY FOR SOCIETY + CYBERSECURITY (CS)

Budget:
~131 Mio. € (CS: 56 Mio. €)
~130 Mio. € (CS: 72 Mio. €)

Weitere Informationen:
www.ffg.at/europa/heu/cluster3

Call Öffnung:
6 May 2026 (CS: 03.03.2026)
5 May 2027 (CS: 02.03.2027)

Kontakt:
Dipl.-Ing. Jeannette Klonk
+43 (0) 57755-4401
jeannette.Klonk@ffg.at

Einreichfrist:
5 November 2026 (CS: 15.09.2026)
4 November 2027 (CS: 15.09.2027)

CL3 – CALL DETAILS 2026/2027

>> DESTINATIONS/TOPICS/BUDGET

Fight against Crime and Terrorism (FCT)
6 Topics, ~41 Mio. €
5 Topics, ~37 Mio. €

Increased Cybersecurity (CS)
3 Topics, 56 Mio. €
4 Topics, 72 Mio.€

Border Management (BM)
3 Topics, 21 Mio.€
3 Topics, 30 Mio.€

Disaster Resilient Society (DRS)
5 Topics, 33 Mio. €
4 Topics, 31 Mio.€

Resilient Infrastructure (INFRA)
3 Topics, 23 Mio. €
2 Topics, 20 Mio.€

Strengthening Security Research and Innovation (SSRI)
4 Topics, 14 Mio. €
3 Topics, 12 Mio.€

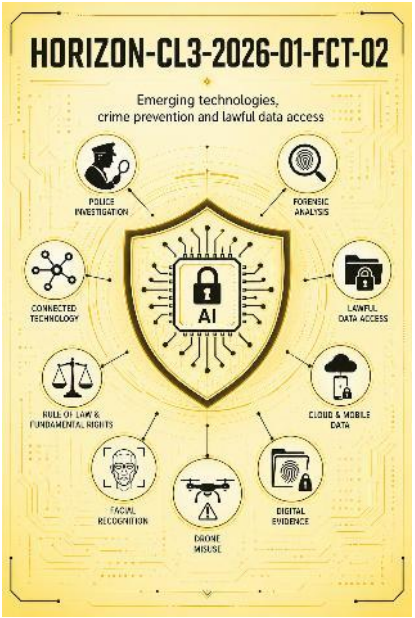
FIGHT AGAINST CRIME AND TERRORISM (FCT)

>> HORIZON-CL3-2026-01-FCT-02

Open topic on preventing and countering the misuse of emerging technologies for criminal purposes, including issues related to lawful access to data (RIA)

Ziele:

- Entwicklung neuer Werkzeuge und Methoden für Polizeibehörden zur Bekämpfung des kriminellen Missbrauchs neuer Technologien wie KI, Quanten- oder Kommunikationstechnologien.
- Unterstützung eines rechtmäßigen Zugangs zu digitalen Daten unter Wahrung von Datenschutz, Privatsphäre und Grundrechten.
- Stärkung der Zusammenarbeit zwischen Polizei, Technologieentwicklern und Politik zur Entwicklung gemeinsamer europäischer Ansätze und Trainings.
- …



KI-generiert mit ChatGPT

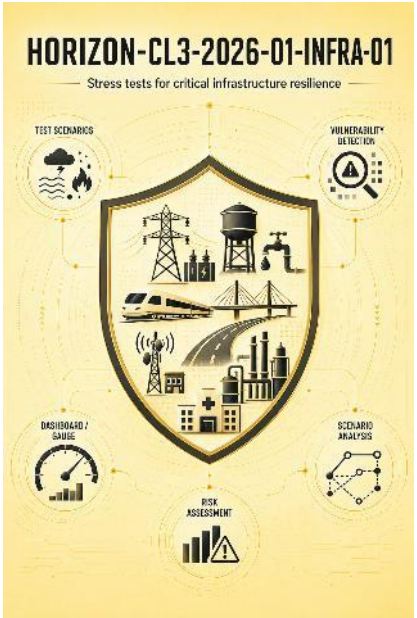
RESILIENT INFRASTRUCTURE (INFRA)

>> HORIZON-CL3-2026-01-INFRA-01

Tools and processes to support stress tests of critical infrastructure (IA)

Ziele:

- Entwicklung von Werkzeugen und Prozessen zur Durchführung von Stresstests kritischer Infrastrukturen gegenüber physischen, hybriden und cyberbezogenen Bedrohungen.
- Verbesserung der Resilienz kritischer Einrichtungen durch realistische Risikoanalysen, Simulationen und Szenarien.
- Unterstützung von Betreibern und Behörden bei der Identifikation von Schwachstellen sowie bei der Vorbereitung auf Krisen und Ausfälle.
- …



KI-generiert mit ChatGPT

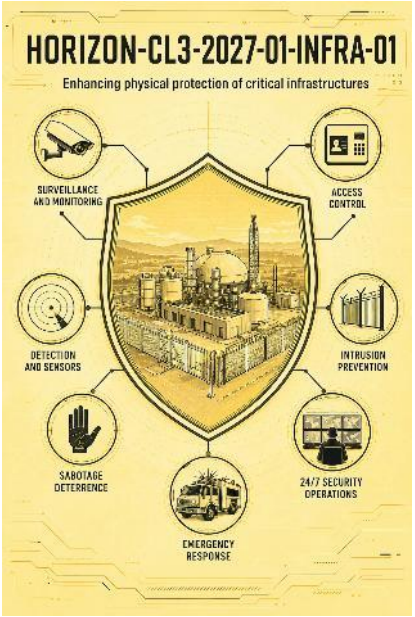
RESILIENT INFRASTRUCTURE (INFRA)

>> HORIZON-CL3-2027-01-INFRA-01

Enhancing physical protection of critical infrastructures (IA)

Ziele:

- Entwicklung innovativer Lösungen zum besseren physischen Schutz kritischer Infrastrukturen gegen Bedrohungen wie Sabotage, Terrorismus oder hybride Angriffe.
- Verbesserung der Prävention, Erkennung und Reaktion auf Angriffe durch neue Technologien, Sicherheitskonzepte und Schutzmaßnahmen.
- Stärkung der Resilienz kritischer Einrichtungen und Unterstützung von Betreibern und Behörden bei Sicherheits- und Krisenmanagement.
- …



KI-generiert mit ChatGPT

RESILIENT INFRASTRUCTURE (INFRA)

>> HORIZON-CL3-2027-01-INFRA-02

Impact of malicious use of Open-Source Intelligence on critical infrastructure business continuity (IA)

Ziele:

- Untersuchung der Auswirkungen des missbräuchlichen Einsatzes von Open-Source-Intelligence (OSINT) auf die Geschäftskontinuität kritischer Infrastrukturen.
- Entwicklung von Methoden und Werkzeugen zur Erkennung, Prävention und Abwehr von Bedrohungen, die durch öffentlich verfügbare Informationen entstehen können.
- Unterstützung von Betreibern kritischer Infrastrukturen beim Schutz sensibler Informationen sowie bei Resilienz- und Krisenmanagementmaßnahmen..
- …

KI-generiert mit ChatGPT

STRENGTHENING SECURITY RESEARCH AND INNOVATION (SSRI)

>> HORIZON-CL3-2026-01-SSRI-04

Development of ecosystem and next-generation capabilities for a secured European Critical Communication System in civil security (IA)

Ziele:

- Weiterentwicklung eines sicheren europäischen Kommunikationssystems für Behörden und Einsatzkräfte im Bereich der zivilen Sicherheit.
- Aufbau eines europäischen Ökosystems und neuer interoperabler Fähigkeiten für eine sichere und resiliente Kommunikation in Krisen- und Sicherheitslagen.
- Unterstützung der Zusammenarbeit zwischen Behörden, Einsatzorganisationen, Industrie und Forschung zur Stärkung strategischer europäischer Souveränität im Bereich sicherer Kommunikation.
- …

KI-generiert mit ChatGPT

Increased Cybersecurity (CS)

>> HORIZON-CL3-2026-02-CS-ECCC-01

Calls restricted per Art. 22(5) – HEU Reg. (EU) 2021/695

Approaches and tools for security in software and hardware development and assessment (RIA)

Ziele:

- Entwicklung neuer Ansätze und Werkzeuge für mehr Sicherheit bei der Entwicklung und Bewertung von Software- und Hardware-Systemen.
- Verbesserung der Cybersicherheit entlang des gesamten Entwicklungsprozesses, einschließlich Tests, Bewertung und Absicherung kritischer Komponenten.
- Stärkung der europäischen technologischen Souveränität durch sichere, vertrauenswürdige und resiliente digitale Technologien und Entwicklungsumgebungen.
- …

KI-generiert mit ChatGPT

Increased Cybersecurity (CS)

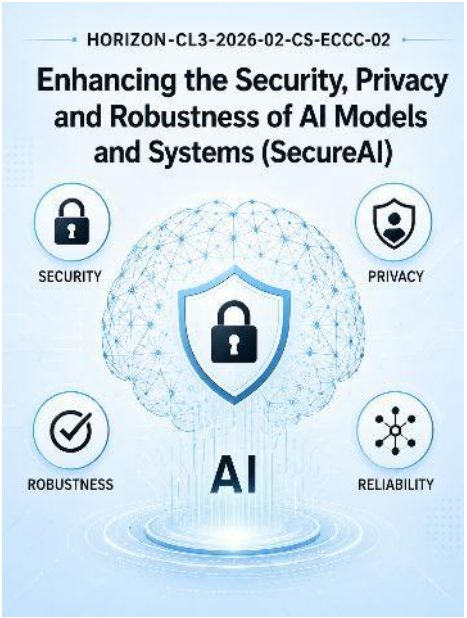
>> HORIZON-CL3-2026-02-CS-ECCC-02

Calls restricted per Art. 22(5) – HEU Reg. (EU) 2021/695

Enhancing the Security, Privacy and Robustness of AI Models and Systems (IA)

Ziele:

- Entwicklung robuster, sicherer und vertrauenswürdiger KI-Systeme mit verbessertem Schutz vor Cyberangriffen, Manipulation und Missbrauch.
- Stärkung von Datenschutz, Resilienz und Zuverlässigkeit von KI-Modellen und KI-basierten Anwendungen in sicherheitskritischen Bereichen.
- Förderung europäischer Kompetenzen und Technologien für sichere KI sowie Unterstützung der praktischen Umsetzung und Validierung entsprechender Lösungen.
- …



KI-generiert mit ChatGPT

Increased Cybersecurity (CS)

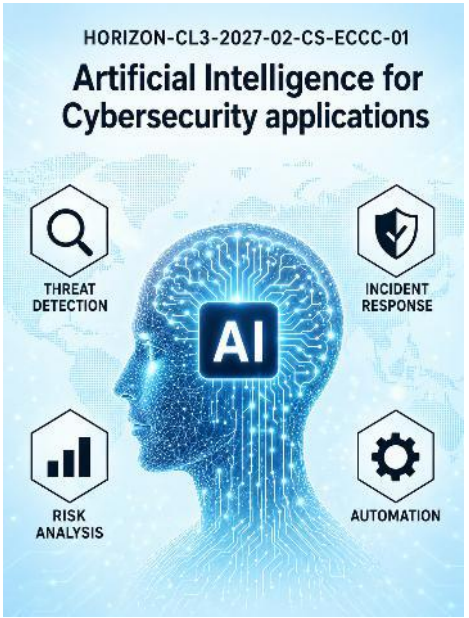
>> HORIZON-CL3-2027-02-CS-ECCC-01

Calls restricted per Art. 22(5) – HEU Reg. (EU) 2021/695

Artificial Intelligence for Cybersecurity applications (RIA)

Ziele:

- Entwicklung von KI-basierten Anwendungen zur Verbesserung der Cybersicherheit, etwa für Angriffserkennung, Bedrohungsanalyse und automatisierte Reaktion auf Cybervorfälle.
- Stärkung der Resilienz digitaler Systeme durch den Einsatz vertrauenswürdiger, sicherer und leistungsfähiger KI-Technologien.
- Förderung europäischer Kompetenzen und Innovationen im Bereich „AI for Cybersecurity“, um Europas technologische Souveränität und Wettbewerbsfähigkeit zu stärken.
- …



KI-generiert mit ChatGPT

Increased Cybersecurity (CS)

>> HORIZON-CL3-2027-02-CS-ECCC-02

Calls restricted per Art. 22(5) – HEU Reg. (EU) 2021/695

Secure Computing Continuum (IoT, Edge, Cloud, Data spaces) (IA)

Ziele:

- Entwicklung sicherer Lösungen für das „Secure Computing Continuum“ über IoT-, Edge-, Cloud- und Datenraum-Technologien hinweg.
- Verbesserung von Cybersicherheit, Datenschutz und Vertrauenswürdigkeit verteilter digitaler Infrastrukturen und Dienste.
- Stärkung interoperabler und resilienter europäischer Technologien zur sicheren Verarbeitung und Nutzung von Daten in vernetzten Umgebungen.
- …

KI-generiert mit ChatGPT

Increased Cybersecurity (CS)

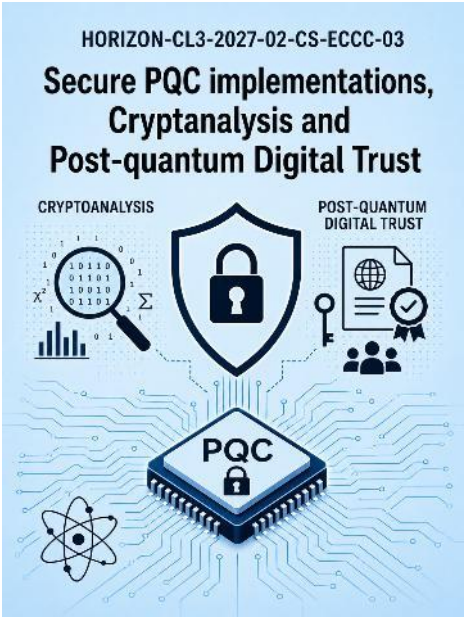
>> HORIZON-CL3-2027-02-CS-ECCC-03

Calls restricted per Art. 22(5) – HEU Reg. (EU) 2021/695

Secure PQC implementations, Cryptanalysis and Post-quantum Digital Trust (RIA)

Ziele:

- Entwicklung sicherer Post-Quanten-Kryptographie (PQC) und hochsicherer kryptographischer Implementierungen für zukünftige digitale Infrastrukturen.
- Verbesserung der Widerstandsfähigkeit europäischer Systeme gegenüber zukünftigen Quantenangriffen durch Kryptanalyse und neue Vertrauensmechanismen.
- Förderung europäischer Kompetenzen und Technologien im Bereich quantensicherer digitaler Vertrauensdienste und sicherer Kommunikation.
- …



KI-generiert mit ChatGPT

SYNERGIEPROGRAMME

DIGITAL EUROPE

DIGITAL EUROPE PROGRAMME

<u>Ziele von DIGITAL</u>: Den digitalen Wandel in Europa vorantreiben

- Digital Europe fördert <u>keine</u> Forschung
- Zielgruppen sind über F&E Community hinausgehend
- Unterstützung von Services für KMU und öffentliche Verwaltung

<u>Aktuelle Möglichkeiten</u>

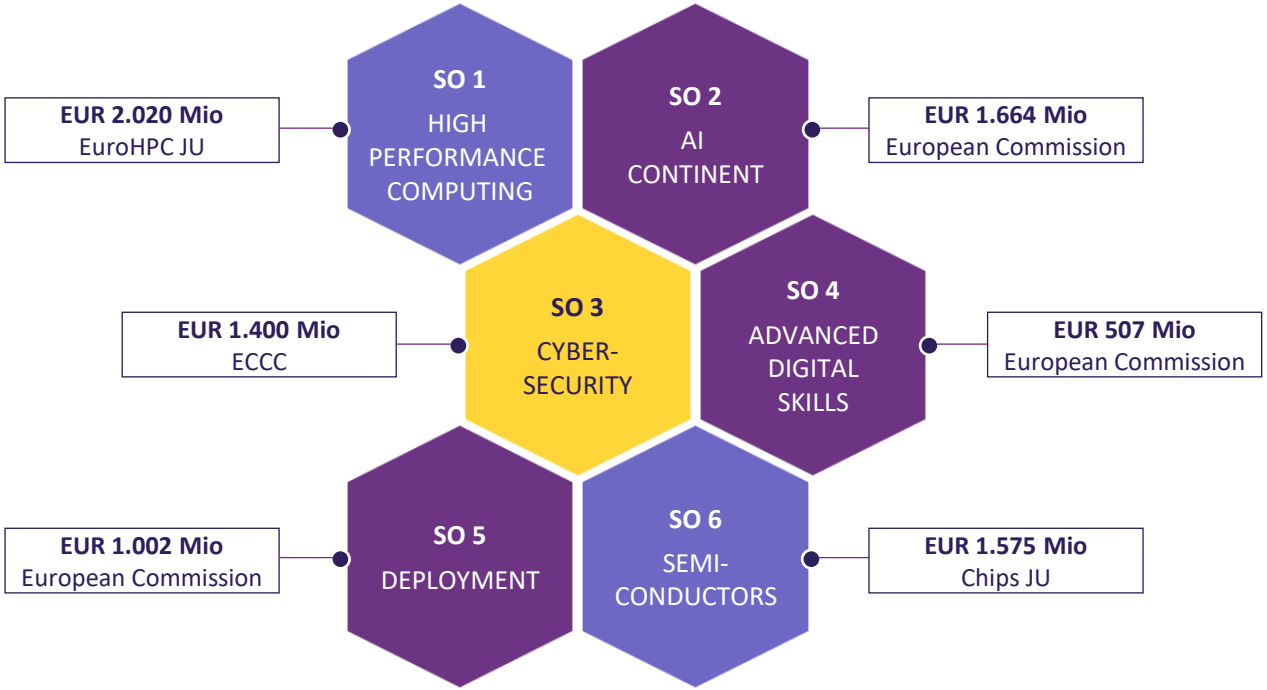
- 10. Call im Hauptarbeitsprogramm ist noch bis 1. Oktober geöffnet
- Aufbau von Sectoral Digital Skills Academy for Semiconductors (2027)
- Auch für die aktuellen & zukünftigen Calls gibt es die Möglichkeit zur nationalen Ko-Finanzierung → frühzeitige Kontaktaufnahme mit DIGITAL NCPs!

National Contact Points

- **Max ARENDS**
  max.arends@ffg.at
- **Daniela HACKL**
  daniela.hackl@ffg.at
- **Patricia TRINKL**
  patricia.trinkl@ffg.at

DIGITAL EUROPE PROGRAMME

>> THEMENSCHWERPUNKTE UND ARBEITSPROGRAMME



Ziele & Abgrenzung

- Den Digitalen Wandel vorantreiben
- Digital Europe unterstützt Services für KMU und öffentliche Verwaltung
- Digital Europe investiert in Bereichen von allg. Interesse und wo der Markt „versagt“
- Zielgruppen des DIGITAL sind über F&E Community hinausgehend
- Digital Europe fördert KEINE Forschung!

DIGITAL EUROPE PROGRAMME

>> 10. Call im Hauptarbeitsprogramm

SO	Thema	Budget [Mio €]	Instrument	Förderrate EK
SO2	Digital solutions for regulatory compliance through data	8,5	Lump Sum	50%
	Apply AI: Piloting AI-based image screening in medical centres	9	Simple Grant	50%
SO4	Advanced Digital Skills for AI Uptake in Health	7,8	Lump Sum	50%
	Digital Skills and Jobs Platform: The National Coalitions for Digital Skills and Jobs	2	CSA	100%
	EdTech accelerator	2,7	CSA	100%
SO5	Building capacity to deploy the EEHRxF and digital health services and systems to support the rights of citizens and reuse of health data under EHDS	14,4	GFS	100%
	Ensuring comprehensive geographical coverage of the Network of Safer Internet Centres (SICs)	10	Simple Grant	50%
	Research Support Framework for Situational Awareness on information integrity	6	GFS	100%
	Support to the implementation of Multi-Country Projects (MCPs)	1	Lump Sum	50%
	Support to Dissemination and Exploitation (D&E) for the Digital Europe Programme	1,8	CSA	100%

DIGITAL EUROPE PROGRAMME

>> Ausblick 2027

SO	Thema	Budget [Mio €]	Instrument	Förderrate EK
SO2	Reference deployments of European Cloud-edge Services	9	Lump Sum	50%
	Data Space for Tourism	6,8	SME Support Action	50% bzw. 75% KMU
	Data Space for Skills	3,5	Simple Grant	50%
	Testing GenAI4EU applications at scale and under real-world conditions	16	Simple Grant	50%
	Virtual Human Twins and Artificial Intelligence in health: Platform validation and uptake incubator	7,2	Lump Sum	50%
SO4	Sectoral digital skills academies – Semiconductor Skills Academy	9	Lump Sum	50%
	Excellence in higher education and training programmes in key digital areas	20,3	Lump Sum	50%
	Supporting the coordination of the Cybersecurity Skills Academy	1	CSA	100%
	Digital Infrastructure for schools and training institutions	10	CSA	100%
SO5	Support to the implementation of Multi-Country Projects (MCPs)	19,5	Lump Sum	50%

SYNERGIEPROGRAMME

European Cybersecurity Competence Centre (ECCC) &
National Cybersecurity Competence Centre (NCC-AT)

DIGITAL EUROPE – CYBERSECURITY

>> ARBEITSPROGRAMM 2025-2027

Calls restricted per Art. 12(5) – DEP Reg. (EU) 2021/694

Cybersecurity

Implementiert durch ECCC

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cyber Resilience Act | **Cyber Solidarity Act** | **NIS2 Directive**

New Technologies, AI & Transition to Post-Quantum

Development and Implementation of AI Tools, SME Support, Post-Quantum Transition

Cyber Solidarity Act Implementation

National and Cross-Border Cyber Hubs, Ecosystem & Information Sharing, Preparedness Testing

Additional Actions for Improving EU Cyber Resilience

NCC Network, Healthcare, Legislative Compliance, Dual-Use Technologies

DIGITAL EUROPE PROGRAMME

>> Ausblick 11. Call im Arbeitsprogramm Cybersecurity (09/2026)

Thema	Budget [Mio €]	Instrument	Förderrate EK
Cybersecure tools, technologies and services relying on AI	15	Simple Grant	50%
Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions	20	SME Support Action	75%/ 50%
National Cyber Hubs	5	Simple Grant	50%
Strengthening the Cyber Hubs ecosystem and enhancing information sharing	2	CSA	100%
Coordinated preparedness testing and other preparedness actions	15	Simple Grant	50%
Mutual assistance	2	Simple Grant	50%
Regional Cable Hubs	5	Simple Grant	70%
Enhancing the NCC Network	11	Simple Grant	50%
Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements	20	Simple Grant	50%
Dual-use technologies	10	Simple Grant	50%

Kontakt:

Nationales Koordinierungszentrum Cybersicherheit (NCC-AT)

DIGITAL Europe - Cybersecurity

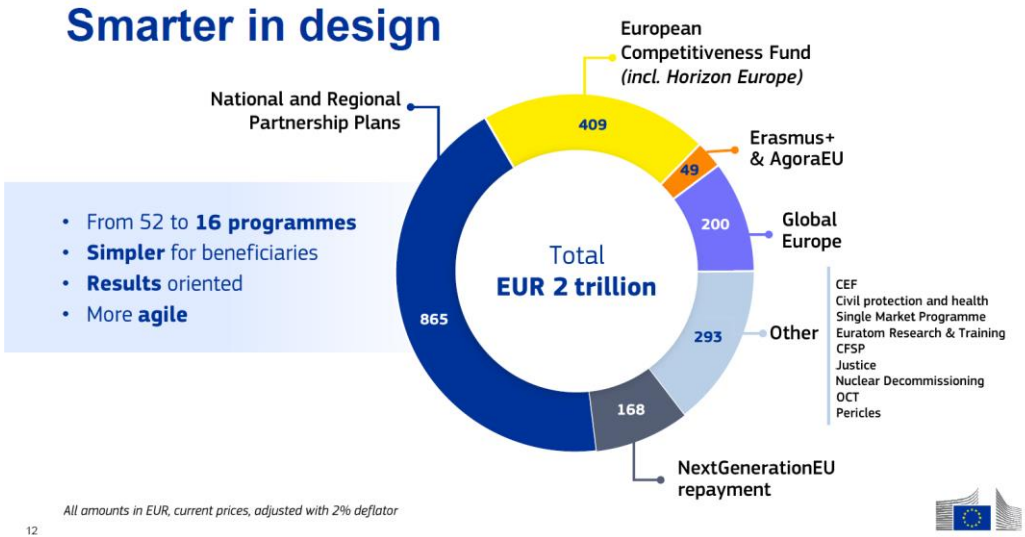
Anja Klauzer, MSc
anja.klauzer@ffg.at

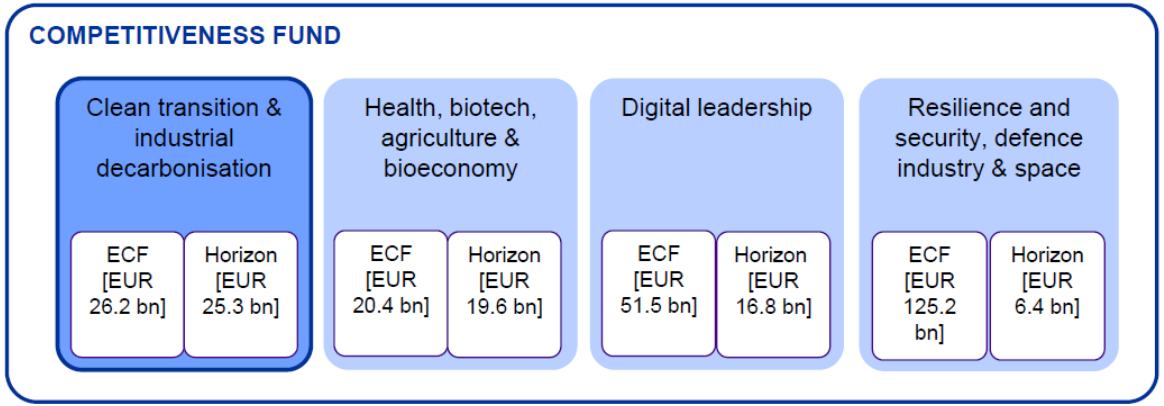
DI Lydia Lindner, BSc.
lydia.lindner@ffg.at

AUSBLICK HORIZON EUROPE HEU 2028+

MFF 2028-2034

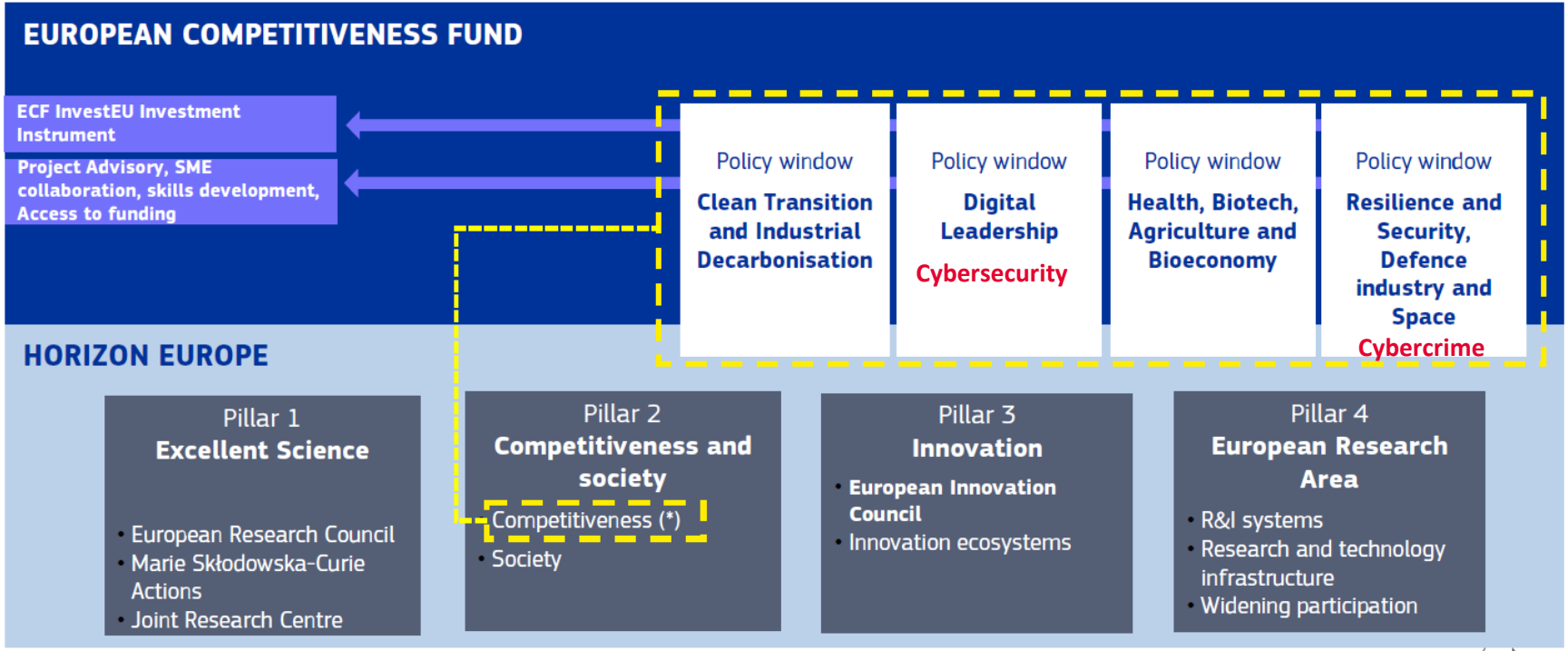
Vorschlag vom 16.6.
Verhandlungen ECF: seit September ´25
Verhandlungen Horizon Europe: seit Oktober ´25





- größte Veränderung **Verschränkung von Horizon Europe und dem Europäischen Wettbewerbsfond** (ECF) in den vier „Policy Windows“

HEU UND ECF ARCHITEKTUR



* Consistent with activities of the European Competitiveness Fund

UNSERE SERVICES

FFG – UNSERE SERVICES

Wir beraten Sie gerne
per E-Mail, Telefonanruf und auch persönlich

Überprüfung Ihrer Projektidee
Senden Sie uns Ihren "One Pager" und wir besprechen die Idee per Telefon oder Videoanruf

Proposalcheck
Persönliche Beratung sowie schriftliches Feedback zu Ihrem Antrag

FFG Academy Trainings
https://www.ffg.at/europa/akademie

Registrieren Sie sich für unsere Newsletter
https://www.ffg.at/ffg-newsletter-2026

Join the community
Website, Newsletter, Veranstaltungen
→ auf dem Laufenden bleiben!
https://horizon-europe-community.at/

DANKE FÜR IHRE AUFMERKSAMKEIT!

Dipl-Ing Jeannette Klonk
Nationale Kontaktselle (NCP)
Zivile Sicherheit für die Gesellschaft

Österreichische Forschungsförderungsgesellschaft
Sensengasse 1, A-1090 Wien

T +43 (0) 5 77 55 – 4401
M +43 (0) 664 88 963003
jeannette.klonk@ffg.at
www.ffg.at