Digitális Biztonság a Horizont 2020 Információs és Kommunikációs Technológiák pályázatokban

Information & Communication Technologies

Edina Németh – ICT, FET

Horizon 2020 Programme Committee Member (PC)
National Contact Point (NCP)

Biztonságos társadalom információs nap

Content

- ICT & Security calls for proposals
  - Horizon 2020 ICT Calls, Societal Challenge 7 Calls
  - Financial Support for Third parties (a.k.a. Cascade funding)
- Digital in the next MFF (2021 – 2027)
- National Contact Points
- ICT Proposers' Day 2019 – Helsinki, Finland

European Commission

Horizon 2020

Information and Communication Technologies & Security

HORIZON 2020

Budget per priority for ICT

Egyszerűsítés?

ICT & Security in H2020

Excellent Science

Frontier Research (ERC)

Future and Emerging Technologies (FET) ICT

Skills and career development (Marie Skłodowska-Curie)

Research Infrastructures ICT

Industrial Leadership

Leadership in enabling

and industrial technologies

ICT ICT ICT

Nanotech., Materials, Manuf. & Processing

Biotechnology

Space ICT

Access to risk finance

Innovation in SMEs

Societal Challenges

Health, demographic change and wellbeing ICT

Food security, sustainable agriculture, and the bio-based economy ICT

Secure, clean and efficient energy ICT

Smart, green and integrated transport ICT

Climate action, resource efficiency, and raw materials ICT

Inclusive, innovative and reflective societies

Secure societies ICT ICT

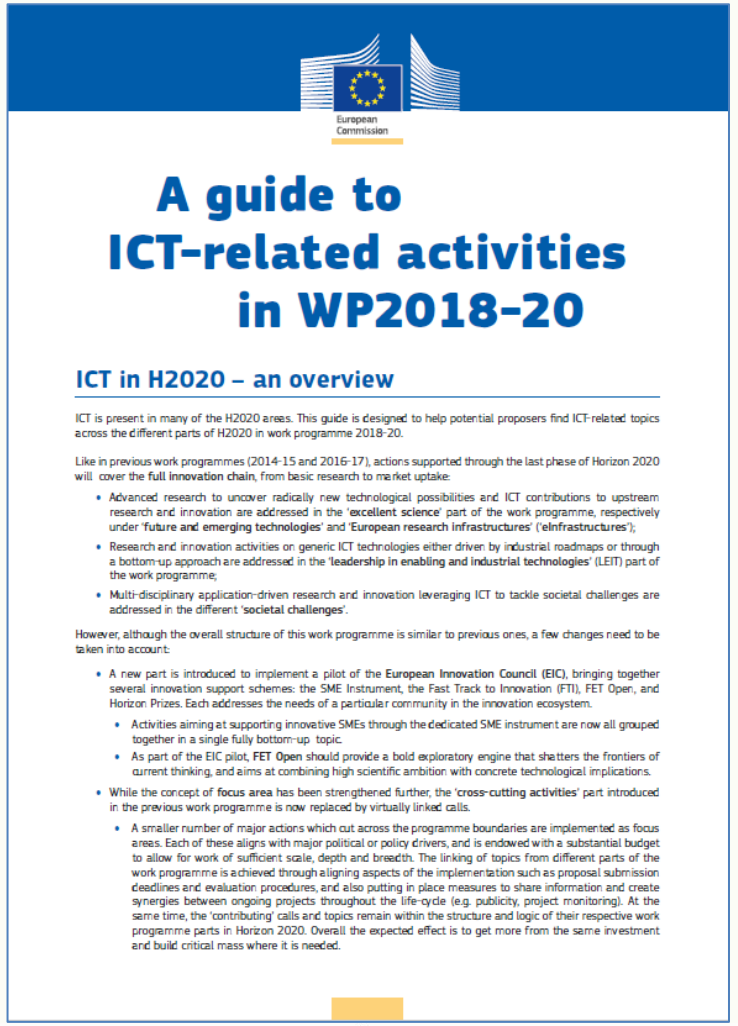
Hol találunk IKT & digitalis biztonsággal kapcsolatos pályázatokat a H2020-ban?

Minden területen!

új megközelítés

Guide to ICT-related activities in WP

- **Comprehensive coverage of the three H2020 pillars**
- **Detailed list of calls and topics**
- **Available on H2020 website**



European Commission

A guide to ICT-related activities in WP2018-20

ICT in H2020 – an overview

ICT is present in many of the H2020 areas. This guide is designed to help potential proposers find ICT-related topics across the different parts of H2020 in work programme 2018-20.

Like in previous work programmes (2014-15 and 2016-17), actions supported through the last phase of Horizon 2020 will cover the **full innovation chain**, from basic research to market uptake:

- Advanced research to uncover radically new technological possibilities and ICT contributions to upstream research and innovation are addressed in the '**excellent science**' part of the work programme, respectively under '**future and emerging technologies**' and '**European research infrastructures**' ('**eInfrastructures**');
- Research and innovation activities on generic ICT technologies either driven by industrial roadmaps or through a bottom-up approach are addressed in the '**leadership in enabling and industrial technologies**' (LEIT) part of the work programme;
- Multi-disciplinary application-driven research and innovation leveraging ICT to tackle societal challenges are addressed in the different '**societal challenges**'.

However, although the overall structure of this work programme is similar to previous ones, a few changes need to be taken into account:

- A new part is introduced to implement a pilot of the **European Innovation Council (EIC)**, bringing together several innovation support schemes: the SME Instrument, the Fast Track to Innovation (FTI), FET Open, and Horizon Prizes. Each addresses the needs of a particular community in the innovation ecosystem.
  - Activities aiming at supporting innovative SMEs through the dedicated SME instrument are now all grouped together in a single fully bottom-up topic.
  - As part of the EIC pilot, **FET Open** should provide a bold exploratory engine that shatters the frontiers of current thinking, and aims at combining high scientific ambition with concrete technological implications.
- While the concept of **focus area** has been strengthened further, the '**cross-cutting activities**' part introduced in the previous work programme is now replaced by virtually linked calls.
  - A smaller number of major actions which cut across the programme boundaries are implemented as focus areas. Each of these aligns with major political or policy drivers, and is endowed with a substantial budget to allow for work of sufficient scale, depth and breadth. The linking of topics from different parts of the work programme is achieved through aligning aspects of the implementation such as proposal submission deadlines and evaluation procedures, and also putting in place measures to share information and create synergies between ongoing projects throughout the life-cycle (e.g. publicity, project monitoring). At the same time, the 'contributing' calls and topics remain within the structure and logic of their respective work programme parts in Horizon 2020. Overall the expected effect is to get more from the same investment and build critical mass where it is needed.

European Commission

Horizon 2020

Information and Communication Technologies & Security

in WP2019

HORIZON 2020

Description of the topics

- 3 key features in Work Programme
  - ***Specific Challenge*** – sets the context, the problem to be addressed, why intervention is necessary
  - ***Scope*** – delineates the problem, specifies the focus and the boundaries of the potential action BUT without overly describing specific approached
  - ***Expected Impact*** – describes the key elements of what is expected to be achieved
- Simplified types of action (instruments): Research & Innovation 100%; Innovation 70%; Coordination and Support Action etc.
- Size of projects may be indicated

Cybersecurity in WP2018-2020

Societal Challenge 7: Secure Societies - Protecting freedom and security of Europe and its citizens:

- **Digital Security (DS) Call**
- **INFRA Call**

LEIT-ICT – part 5.i Information and Communication Technologies:

- **Cybersecurity Call**
- **Cybersecurity measures embedded in several other topics**

SC7 – Digital Security Call - Overview

Topics 2019:

SU-DS03-2019-2020: Digital security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises (IA, Budget: 18 MEUR)

SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors (subtopic a) Transport, IA, budget: 10 MEUR; subtopic b) Healthcare, RIA, budget: 10 MEUR)

Opening: 14 Mar 2019

Call deadline: 22 Aug 2019

SU-DS03-2019-2020: Digital security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises

Subtopics:

(a): Protecting citizens' security, privacy and personal data

(b): Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection

Type of Action: IA

Budget: 18 MEUR

SU-DS03-2019-2020 – Specific Challenge

- Need **to protect freedom, security and privacy**, and ensure **personal data** protection of **Europe's citizens**;
- Citizens should be enabled to **assess risks** of their digital activities and **configure their own settings** and controls;
- Citizens need to be aware of the need of their **informed consent** and become capable in providing their permission/consent;
- **SMEs&MEs** lack sufficient **awareness** and can allocate limited **resources** to counter cyber risks, being easier targets;
- Cybersecurity is a complex and fast-evolving field, and security professionals and experts working for SMEs&MEs need to be in a **constant learning process**;
- tailored research and innovation should support cybersecurity for SMEs&Mes, as they have a **significant economic role in the EU**;

SU-DS03-2019-2020: Expected Impact

- **Citizens and SMEs&MEs** better protected, becoming active players in the **Digital Single Market**, including implementation of NIS directive and GDPR application.
- **Security, privacy and personal data protection** strengthened as shared responsibility along all layers in the **digital economy**, including citizens and SMEs&MEs.
- Reduced economic damage caused by harmful cyber-attacks, privacy incidents and data protection breaches.
- Pave the way for a **trustworthy EU digital environment** benefitting all economic and social actors.

SU-DS03-2019-2020: Scope - subtopic a) Protecting citizens' security, privacy and personal data

- **Innovative solutions,** including innovative approaches, techniques and **user-friendly** tools;
- **New applications & technologies**, enabling citizens to better monitor and audit their security, privacy and personal data protection, **to become more engaged** and active in the fight against cyber risks;
- Engage end-users by involving them in design and implementation, ensuring usability and acceptability;
- Assurance and transparency;
- Build bridges/synergies with **data protection authorities** and CERTs/CSIRTs.

SU-DS03-2019-2020: Scope - subtopic b) SMEs&Mes, defenders of security, privacy, personal data protection

- Innovative solutions to increase the **knowledge sharing** across SMEs&Mes, between them and larger providers;
- Support user SMEs&MEs by **democratizing access to tools and solutions** of varied sophistication level, to allow them benefit from innovative targeted solutions addressing their specific needs and available resources;
- **Targeted, user-friendly and cost-effective solutions** (dynamically monitor, forecast and assess security, privacy and personal data protection risks; become aware of attacks, vulnerabilities and risks influencing business; manage and forecast security, privacy and personal data protection risks in an easy and affordable way; build on-line collaboration between SMEs&MEs associations and with CERTs/CSIRTs);
- Propose tools and processes to facilitate participation of user **SMEs&MEs in cyber ranges**;

SU-DS05-2018-2019 - Digital security, privacy, data protection and accountability in critical sectors

Subtopics:

(a) Digital security, privacy and personal data protection in multimodal transport

Type of Action: IA

Budget: 10 MEUR

(b) Digital security, privacy and personal data protection in healthcare ecosystem

Type of Action: RIA

Budget: 10 MEUR

SU-DS05-2018-2019: Specific Challenge

- Cybersecurity technologies deployed in several **application domains** - aligned to the specific domain needs, linking the demand and supply sides for such cyber technologies.
- **NIS Directive** – identified **critical sectors/subsectors** from the point of view of cybersecurity needs;
- Need to facilitate engagement of **end-users** towards defining and providing **sector-specific common requirements** about digital security, privacy and personal data protection.
- **Building security, privacy and personal data protection by design** and by default → clearly define principles and standards to protect the critical infrastructures in these sectors and ensure personal data integrity and confidentiality.

SU-DS05-2018-2019: Specific Challenge Transport

- Security to be managed pro-actively **over the system as a whole** - must extend to include interfaces to critical supporting infrastructures (**communication networks** and **satellite systems**).
- Complexity of the transport sector:
    - **diversity** of components that build the solutions in use;
    - very **long lifecycle** of these components.
- Main challenge: to migrate these **solutions, systems, and infrastructures** to a **higher level of cybersecurity**.

SU-DS05-2018-2019: Specific Challenge Healthcare

- ICT enables the sector to provide efficient, effective, cross-border top-quality healthcare services **improving public healthcare**.
- New ways of providing healthcare operations, services and applications, via various **interconnected infrastructures, systems, entities and people**.
- **Personalized medicine** as successful approach in treating diseases: increased complexity of the **pharmaceutical supply chain** and raises the importance of achieving a zero error rate in the supply of personalized medications.
- Cybersecurity is **safety critical** and novel approaches are needed to ensure **traceability** and **zero error** deliveries.
- Health - very sensitive sector → take into account requirements related to data protection legislation.

SU-DS05-2018-2019: Expected Impact

- **Short term:** development of the CSIRT Network; identified relevant generic and specific aspects; advanced holistic systems and innovative proof concepts; advances in state-of-the-art analysis of specific aspects; sound **analysis of cascading effects of specific related cyber threats within the supply chain of the respective critical domains/sectors**; improved cybersecurity information sharing and collaboration among stakeholders, and with CERTs/CSIRTs; more targeted and acceptable security management solutions addressing specificities; trigger the fast adoption of cybersecurity/privacy/personal data protection best practices.
- **Medium term:** better response and recovery technologies and services that will help organizations to significantly **reduce the impact of propagated and cascaded threats**, **vulnerabilities and breaches**; **enhanced protection** against emerging novel advanced threats; improved security governance; greater and more mature EU cybersecurity market; reduce the impact of breaches with various levels of success in penetrating the defenses.

SU-DS05-2018-2019: Expected Impact

- **Long term:**

  Better cybersecurity for **specific standards in the respective critical domains/sectors** addressed, that will trigger fast adoption of best practices in the related industry.

  Established **trust chains among all entities** in the eco-systems of the respective critical domains/sectors addressed.

  Better **implementation** of the relevant **EU legislation** (e.g. NIS, eIDAS, GDPR) in the respective critical domains/sectors addressed.

  Companies/organisations in the respective critical domains/sectors addressed are more willing to promote cyber security, privacy and personal data protection in the whole EU specific ecosystem.

SU-DS05-2018-2019: Scope (general)

- Treat generic aspects for min. 2 critical sectors in NIS Directive:
  - identify common threats and attacks;
  - develop proof of concepts for managing cybersecurity & privacy risks;
- Treat specific aspects for one sector/domain (transport/healthcare):
  - identify specific vulnerabilities, propagation effects, counter measures;
  - develop and test cyber innovation-based solutions;
  - validate solutions in pilots/demonstrators;
- During conception & development, take into account specificities (complexity of infrastructure and their large scale);
- Pilots/demonstrators: encouraged to use relevant transversal cyber infrastructures & capabilities developed in other projects;
- Deliver specific social aspects of digital security related to training (practical, operational, hands-on training);

SU-DS05-2018-2019: Scope for sub-topics - Tackle on at least two of the following items:

Transport:

(1): **Secure access** management **for citizens to all types of vehicles**.

(2): Assurance and protection in **multimodal transport**, addressing **interconnected** threats and propagated vulnerabilities.

(3): **Standardization** (allow quick adoption of best practices).

Healthcare:

(1) Develop **dynamic vulnerability data basis**; build dynamic taxonomies.

(2) Deliver dynamic, evidence-based, sophisticated security, privacy and personal data protection risk assessment **frameworks & tools**.

(3): **Provide collaborative privacy-aware tools**, advise and provide best/good practices about incident handling.

DS Call: Specific requirements

- Consider the relevant **human factor and social aspects** when developing innovative solutions.
- Where relevant, proposals should also describe how the **gender dimension** is taken into account in their content.

(Relevance in particular for SU-DS03-2019-2020.)

- Foresee activities and envisage resources for **clustering** with other projects funded under the respective topics (applies for both topics SU-DS03-2019-2020 and SU-DS05-2018-2019), and with other relevant projects in the field funded by H2020.

Cybersecurity Call in LEIT-ICT - SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems

Subtopics:

(a) Cybersecurity/privacy audit, certification and standardization;

(b) Trusted supply chains of ICT systems;

(c) Designing and developing privacy-friendly and secure software and hardware;

Type of Action: RIA

Budget: 47.00 MEUR

Opening: 25/07/2019

Deadline: 19/11/2019

SU-ICT-02-2020: Specific Challenge

- **Algorithms, software and hardware systems** must be designed taking account from design phase, in a measurable manner, of security, privacy, data protection, accountability, etc.
- Develop mechanisms that **measure the performance of ICT systems** with regards to cybersecurity and privacy;
- **Enhance control and trust** of the consumer of digital products and services with innovative tools aiming to ensure the accountability of the security and privacy levels in the algorithms, in the software, and ultimately in the ICT systems, products and services across the supply chain.

SU-ICT-02-2020: Expected Impact

- Improved **market opportunities**.
- **Increased trust** by developers using/integrating ICT components and end-users of IT systems and services.
- Protect the **privacy of citizens** and **trustworthiness of ICT** .
- Accelerated development and implementation of **certification processes**.
- Development of advanced **cybersecurity products** and **services**, improving trust in the Digital Single Market.
- Use of more harmonized certification schemes, increasing **business cases** for more reliable cybersecurity services.
- **Validation platforms** providing assessments with less effort, assuring better compliance with relevant regulations, standards.

SU-ICT-02-2020: Scope (a) Cybersecurity/privacy audit, certification and standardization

Innovative approaches to:

- **Design & develop:**
  - **automated security validation & testing**, exploiting the knowledge of architecture, code, and development environments;
  - **automated security verification** at code level;
- **Develop:**
  - **mechanisms, key performance indicators and measures** that ease the process of certification at the level of services;
  - **mechanisms to better audit and analyse** open source and/or open license software, and ICT systems with respect to cybersecurity and digital privacy.

Creating information bases to measure & assess security of digital assets.

SU-ICT-02-2020: Scope (b) Trusted supply chains of ICT systems

- develop advanced, evidence based, dynamic **methods & tools** for better forecasting, detecting and preventing propagated vulnerabilities;
- estimate dynamically and accurately supply chain cyber security & privacy risks;
- design and develop security, privacy and accountability **measures & mitigation strategies** for all entities in supply chain,
- design & develop **techniques, methods and tools** to better audit complex algorithms, interconnected ICT components/systems;
- devise **methods** to develop resilient systems out of potentially insecure components;
- devise security assurance **methodologies & metrics** to define security claims for composed systems & certification methods.

SU-ICT-02-2020: Scope (c) Designing and developing privacy-friendly and secure software and hardware

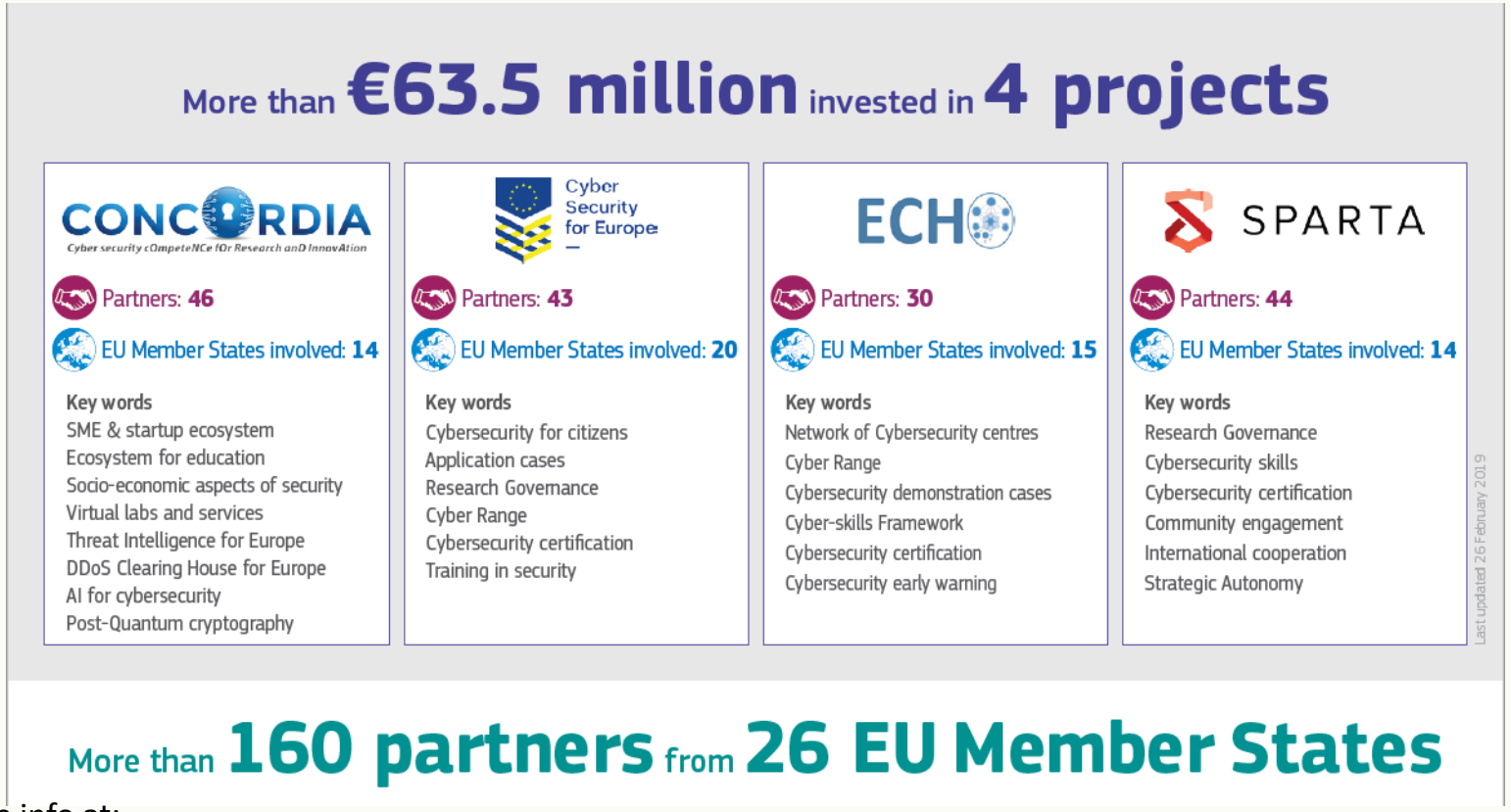
Innovative approaches to establish methods and tools for:

- security and privacy **requirements engineering**;
- embedded algorithmic **accountability**;
- **system-wide consistency** including connection between models, security/privacy/accountability objectives, policies, and functional implementations;
- **metrics** to assess a secure, reliable and privacy-friendly development;
- secure, privacy-friendly and **accountability-enabled programming languages, hardware design languages, development frameworks,** secure compilation and execution;
- novel, secure and privacy-friendly **IoT architectures**.

Other requirements and recommendations

- Consider the relevant **human factor and social aspects** when developing innovative solutions.
- Take account of the **results and work done in other relevant H2020 projects** on cybersecurity/privacy.
- Foresee **actions to collaborate with similar ongoing projects** funded under H2020, in particular with the four projects launched under Horizon2020 LEIT ICT, as a result of the 2018 call for the topic SU-ICT-03-2018 "*Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*"

EU pilots to prepare the European Cybersecurity Competence Network



More info at:
https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

LEIT-ICT - Other topics relevant for Cybersecurity & Digital Privacy

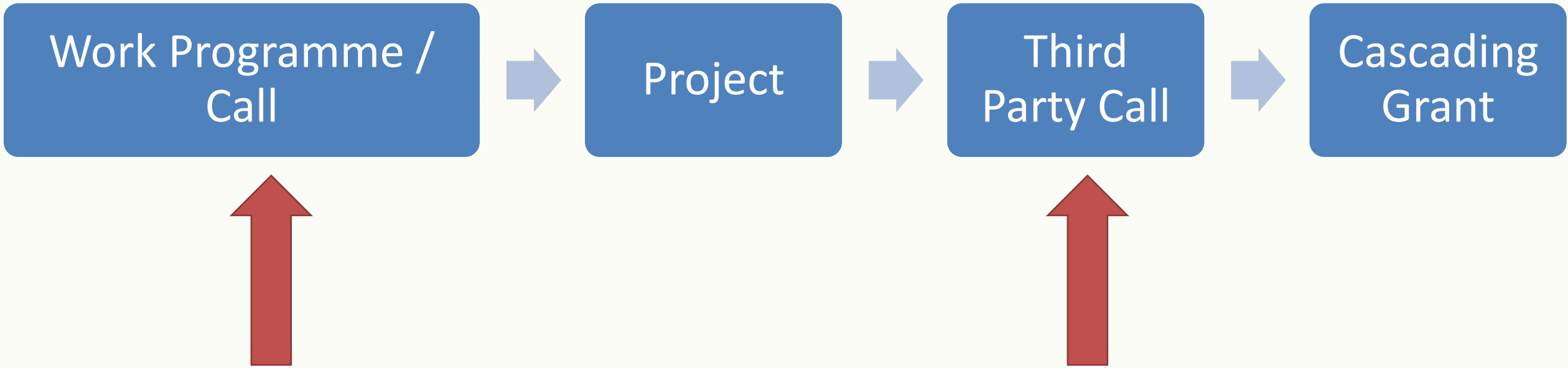
Examples:

- **ICT-08-2019: Security and resilience for collaborative manufacturing environments**
- **ICT-13-2018-2019: Supporting the emergence of data markets and the data economy**
- **ICT-20-2019-2020: 5G Long Term Evolution**
- **…and more, as this is a cross-cutting issue**

Channels for H2020 ICT Funding

- H2020 projects in LEIT (eg. Research and Innovation Actions, Innovation Actions, SME Instrument, FTI projects, Prizes)
- H2020 projects in Societal Challenges (same)
- H2020 projects in Excellent Science (eg. Marie Curie Projects, FET, Infrastructures)
- ECSEL JTI, AAL, ERA-NETs
- Calls for Third Parties / Expressions of Interest through large initiatives (eg. PPP projects, Large Scale Pilots, Smart Anything Everywhere, I4MS, IoT EU platforms, FET Flagships etc.)

Channels for H2020 ICT Funding

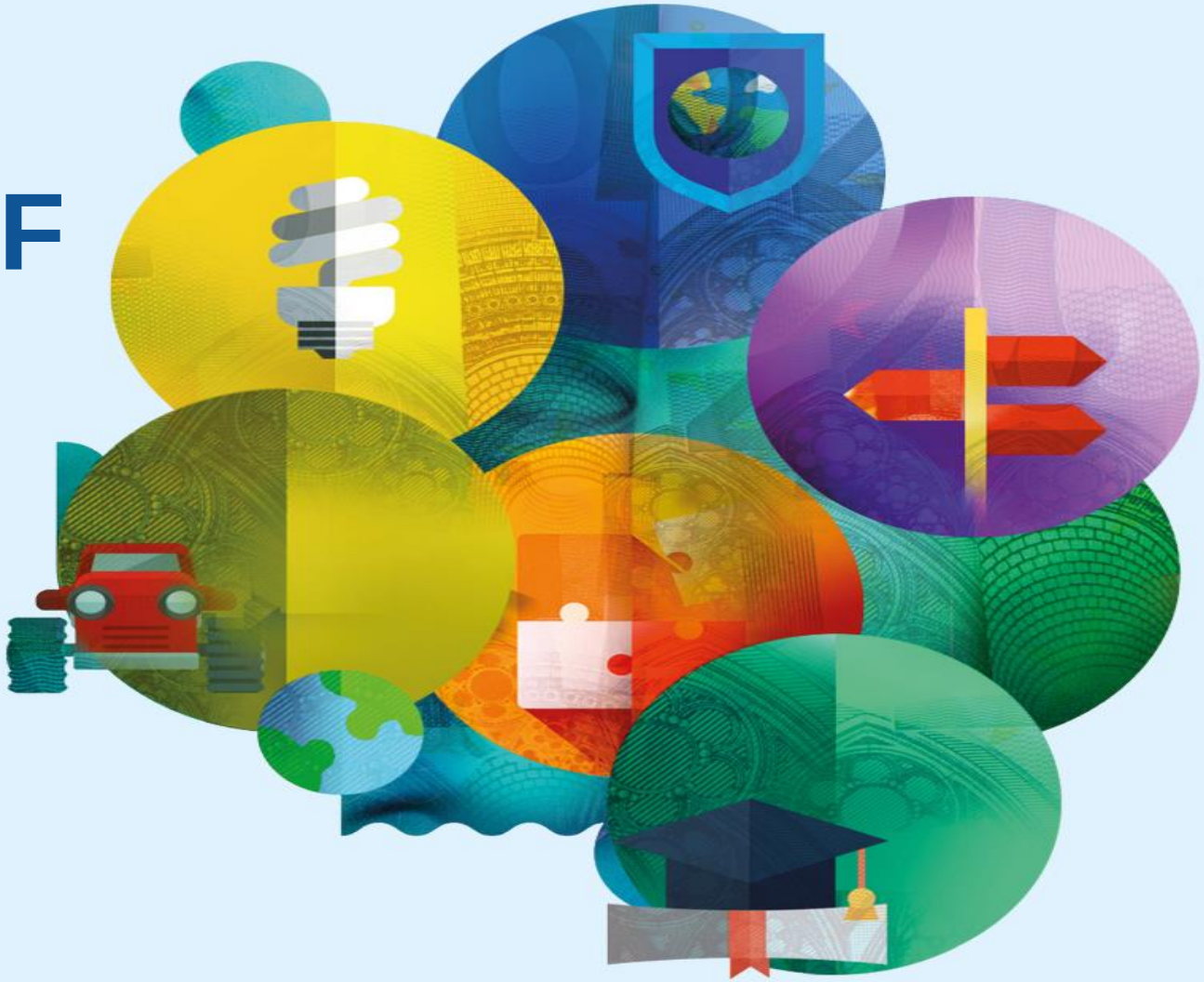


H2020 calls

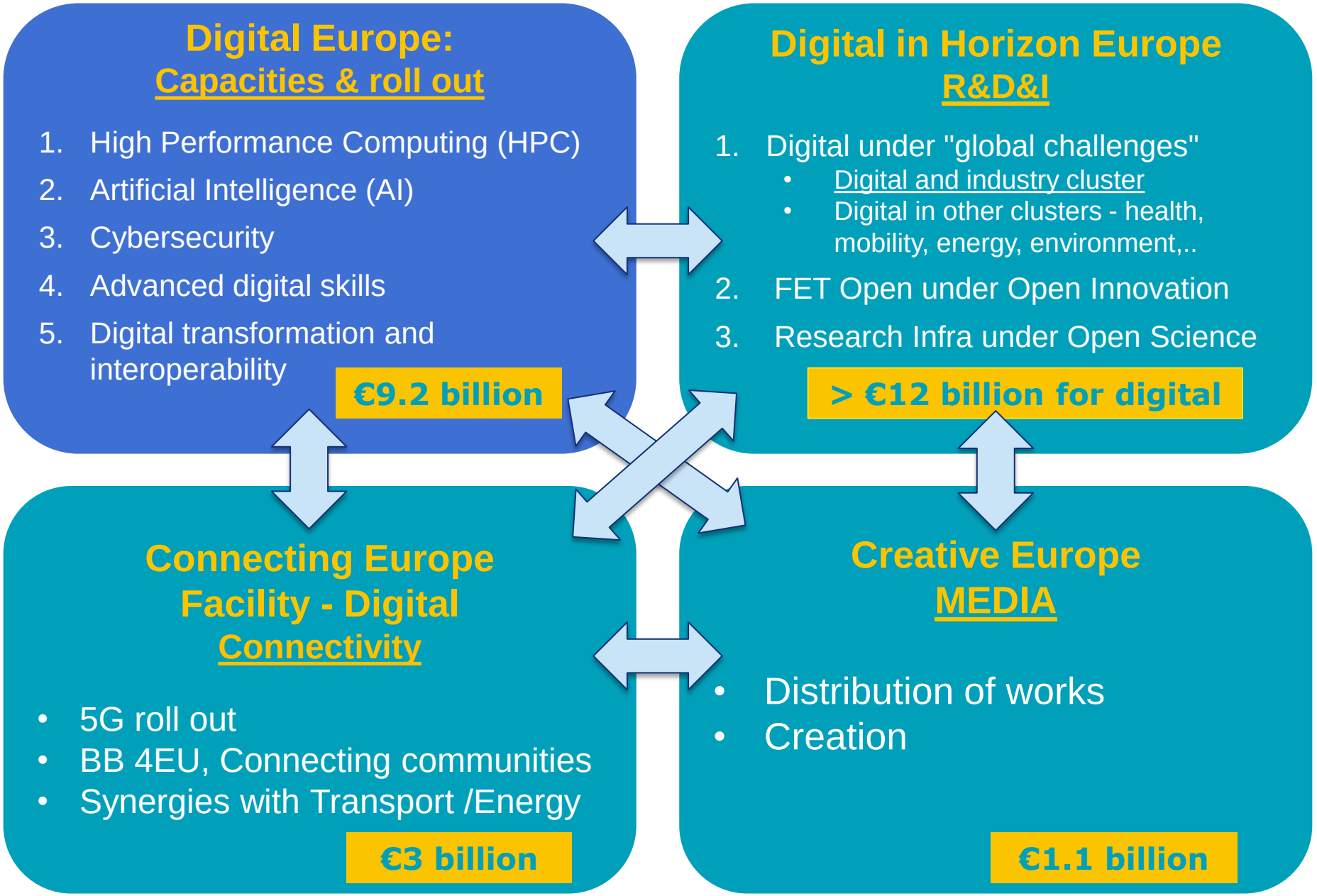
- I4MS – ICT Innovation for Manufacturing SMEs
- SAE - Smart Anything Everywhere
- AI4EU – AI on-demand Platform
- FIRE – Future Internet Research & Experimentation
- FET Flagships – Human Brain, Graphene
- Internet of Things - European Platforms Initiative
- ECHORD++ - The European Coordination Hub for Open Robotics Development
- Pre-commercial procurement (PCP) tenders
- …. Further competitive calls on Funding & Tenders Portal

European Commission

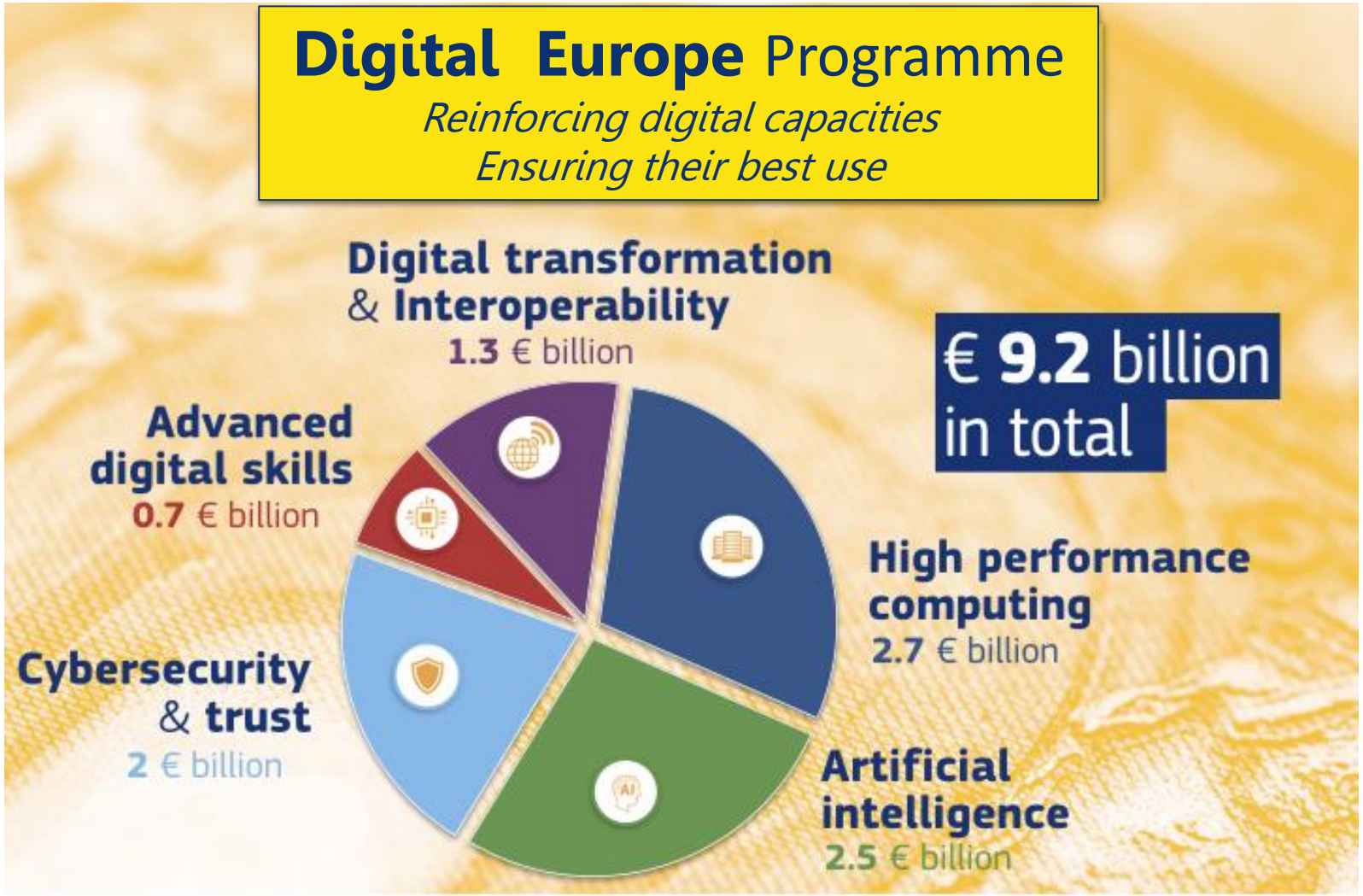
Digital in the next MFF



DIGITAL IN THE NEXT MFF: OVERVIEW

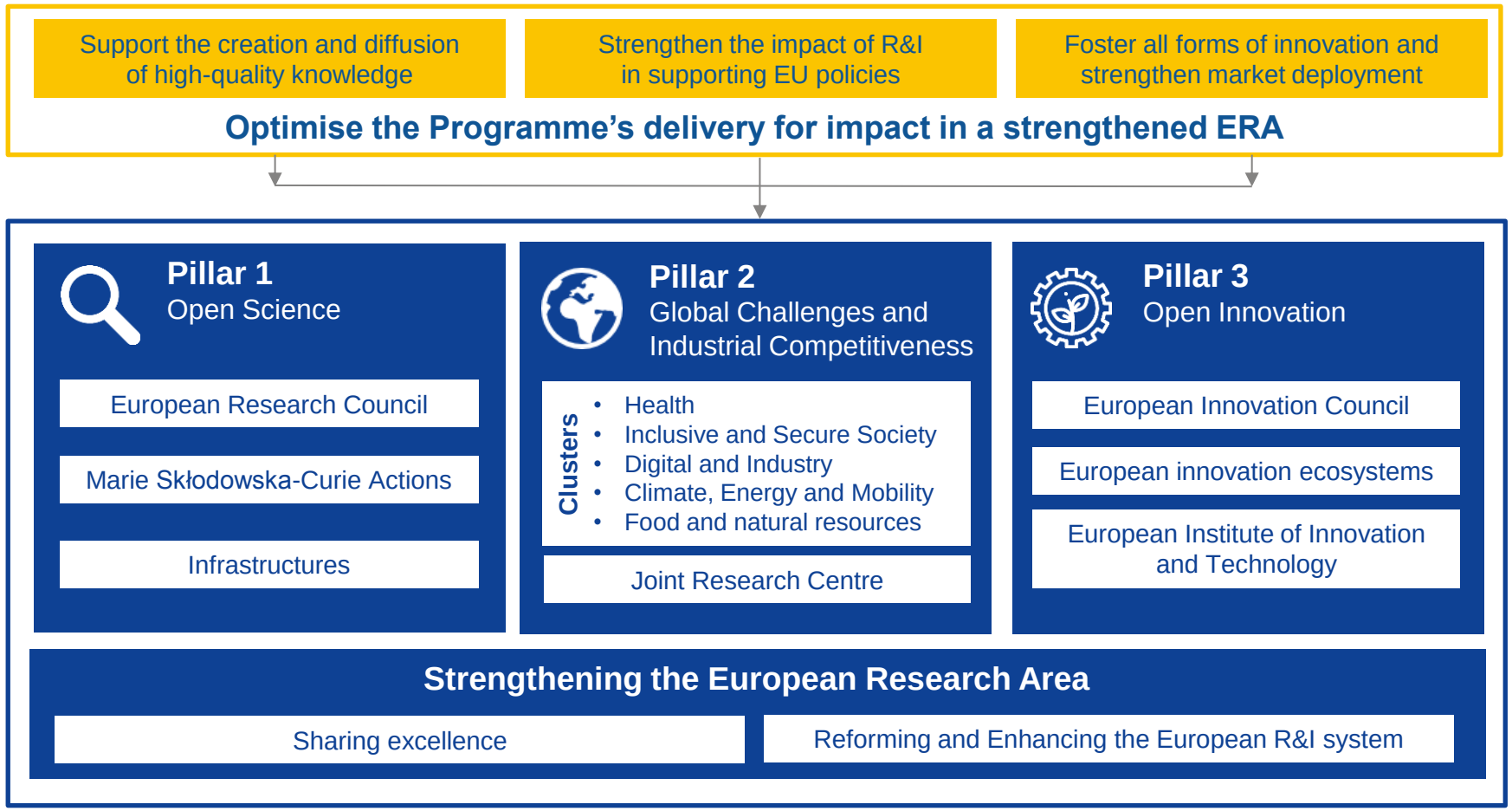


Digital Europe programme – What?



Horizon Europe: evolution not revolution

Specific objectives of the Programme

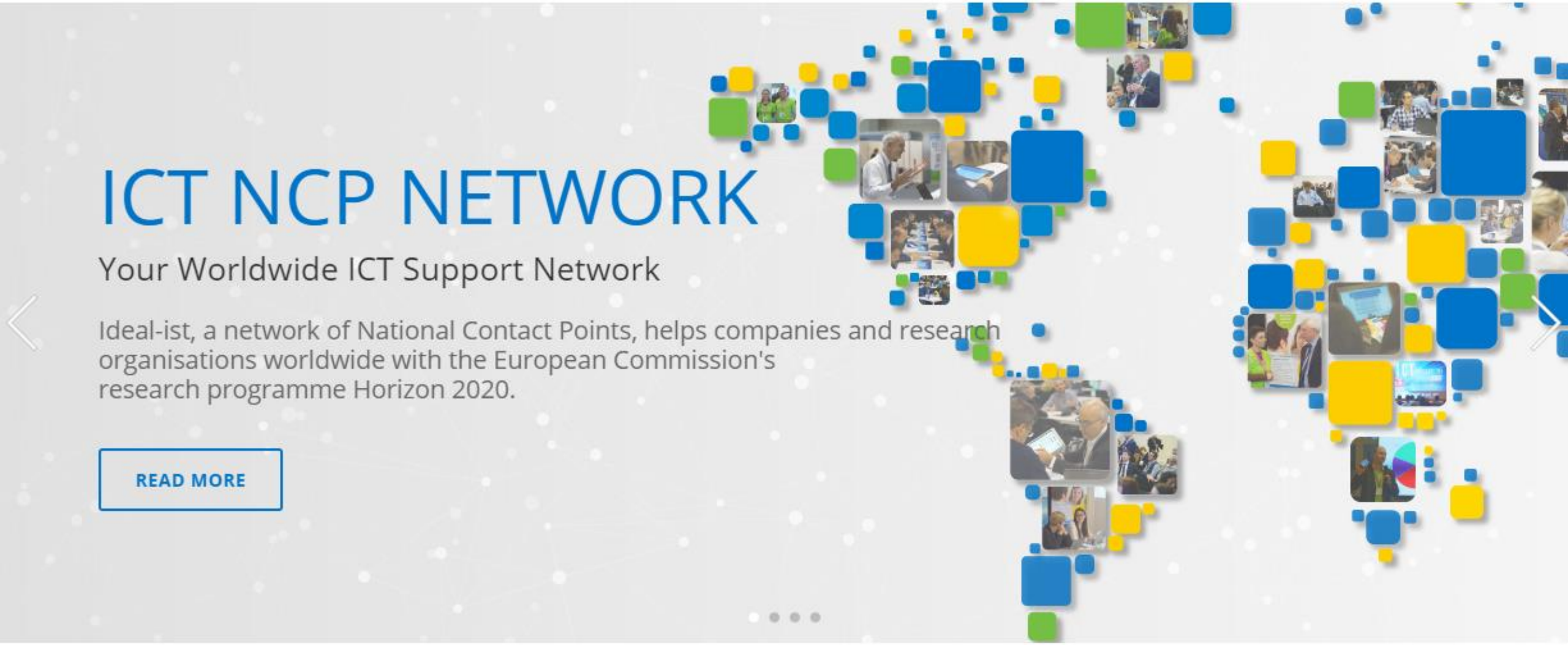


National Contact Point

Partner Search
&
Proposal Development

NCP system in Hungary

- Free information on Horizon 2020 – per thematic area
- Information days: http://nkfih.gov.hu/nemzetkozi-tevekenyseg/horizont-2020-rendezvenynaptar/nkfi-hivatal-h2020
- Electronic / phone / personal information on funding opportunities and processes
- Personal consultations with potential applicants, feedback on project ideas and proposals
- H2020 news, events
- National H2020 website: http://www.h2020.gov.hu/



ICT NCP NETWORK

Your Worldwide ICT Support Network

Ideal-ist, a network of National Contact Points, helps companies and research organisations worldwide with the European Commission's research programme Horizon 2020.

READ MORE

Topic Tree

Partner Search

Toolbox

Pre-proposal Check

ICT Event

19-20 Sep 2019

Helsinki, Finland

INFORMATION – BROKERAGE – CONSORTIUM BUILDING - EXHIBITION

Web: https://ec.europa.eu/digital-single-market/en/news/digital-excellence-forum-ict-proposers-day-2019

Brokerage: https://ict2019.ideal-ist.eu/

Twitter: @DSMeu and #ICTPropDay

Thank you and get in touch !

Németh Edina
ICT & FET
Programme Committee Member
National Contact Point
NKFIH
Edina.Nemeth@ist.hu
+36-70-221-0387