kaila
by zabala

Funding Opportunities Report

DIGITAL EUROPE 2023

INDEX

DIGITAL-2023-CLOUD-AI-04 | Cloud, Data and Artificial Intelligence

1.-DIGITAL-2023-CLOUD-AI-04-IPCEI-EXPLOIT (DIGITAL-CSA) 4
2.-DIGITAL-2023-CLOUD-AI-04-GENOME (DIGITAL-SIMPLE) 6
3.-DIGITAL-2023-CLOUD-AI-04-DEVELOPCITI (DIGITAL-SIMPLE) 8
4.-DIGITAL-2023-CLOUD-AI-04-AEROSEC (DIGITAL-SIMPLE) 10
5.-DIGITAL-2023-CLOUD-AI-04-COORDINATEF (DIGITAL-CSA) 12
6.-DIGITAL-2023-CLOUD-AI-04-ICU-DATA (DIGITAL-SIMPLE) 14

DIGITAL-2023-CLOUD-DATA-04 | Cloud, Data and Artificial Intelligence

7.-DIGITAL-2023-CLOUD-DATA-04-DIGIPASS (DIGITAL-SIMPLE) 16

DIGITAL-2023-DEPLOY-04 | Accelerating the best use of technologies

8.-DIGITAL-2023-DEPLOY-04-EDMO-HUBS (DIGITAL-SME) 17
9.-DIGITAL-2023-DEPLOY-04-NETWORK-OF-SICs (DIGITAL-SIMPLE) 19

DIGITAL-2023-DEPLOY-BESTUSE-TECH-04 | Accelerating the Best Use of Technologies

10. DIGITAL-2023-DEPLOY-BESTUSE-TECH-04-ENERSAVING (DIGITAL-SIMPLE) 21

DIGITAL-2023-PROGRAM-SUPPORT-04 | Programme support actions

11.-DIGITAL-2023-PROGRAM-SUPPORT-04-DISSEM-EXPLOIT (DIGITAL-CSA) 22
12.-DIGITAL-2023-PROGRAM-SUPPORT-04-NETWORK-NCPs (DIGITAL-CSA) 23

DIGITAL-2023-SKILLS-04 | Advanced Digital Skills

13.-DIGITAL-2023-SKILLS-04-BOOSTINGDIGIT (DIGITAL-CSA) 24
14.-DIGITAL-2023-SKILLS-04-SEMICONDUCTORS (DIGITAL-SIMPLE) 25

DIGITAL-ECCC-2023-DEPLOY-CYBER-04 | Deployment actions in the area of cybersecurity

15.-DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE (DIGITAL-JU-CSA) 27
16.-DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION (DIGITAL-JU-SIMPLE) 29
17.-DIGITAL-ECCC-2023-DEPLOY-CYBER-04-STANDARDISATION (DIGITAL-JU-CSA) 30
18.-DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST (DIGITAL-JU-GFS) 31

DIGITAL-ECCC-2022-CYBER-B-03 | Cybersecurity and Trust

19.-DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE (DIGITAL-JU-SME) 32
20.-DIGITAL-ECCC-2022-CYBER-B-03-SOC (DIGITAL-JU-SIMPLE) 34
21.-DIGITAL-ECCC-2022-CYBER-B-03-UPTAKE-CYBERSOLUTIONS (DIGITAL-JU-SME) 35

DIGITAL-2022-CLOUD-AI-B-03 | Cloud, Data and Artificial Intelligence

22.-DIGITAL-2022-CLOUD-AI-B-03-AI-ON-DEMAND (DIGITAL-CSA) 36

Funding Opportunities Report

DIGITAL EUROPE 2023

This document has been generated with Kaila, a platform developed by ZABALA to foster open innovation.

Kaila is a collaborative hub that represents a paradigm shift in the management of innovation ecosystems, using advanced recommendation algorithms and the integration of main EU open data sources.

What can I do with Kaila?

- **Obtain funding for your projects**
- **Analyse innovation trends**
- **Competitive watch**
- **Find partners and collaborators**

Join for free

1. DIGITAL-2023-CLOUD-AI-04-IPCEI-EXPLOIT (DIGITAL-CSA)

Cloud IPCEI Exploitation office

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-CSA DIGITAL Coordination and Support Actions	

Expected Outcome:
The Cloud IPCEI Exploitation Office should provide at minima:
Yearly activity management plans for the pre-notified IPCEI-CIS, including key project deliverables, milestones, risk mitigation measures and a description of roles and responsibilities in form of a RACI matrix. This should build on targeted and granular data collection among IPCEI individual and macro-projects in the context of the upcoming requirements under the Digital Compass and the Recovery and Resilience Facility.A dedicated Cloud IPCEI Exploitation Office website for dissemination purposes with wide reach and a collaborative platform accessible to both IPCEI and non IPCEI participants.A medium-term sustainability roadmap and governance strategy for the pre-notified IPCEI.Key events, meetings and summary reports of the General Assemblies, Board meetings and industrial sessions to be made accessible in the Cloud IPCEI Exploitation Office website.Build a dissemination and exploitation strategy, yearly social media campaigns and the corresponding content to support an active visibility and transparency of the pre-notified IPCEI-CIS activities and technological solutions first industrial deployed and their uptake across all interested stakeholders.

Objective:
This action will support the overall coordination, monitoring, dissemination and long-term exploitation of the activities within the pre-notified Important Project of Common European Interest on Next Generation Cloud and Edge Infrastructure and Services (IPCEI-CIS) via the set-up of a Cloud IPCEI Exploitation Office. The Office's objective is to disseminate the results of this IPCEI and contribute to the exploitation and re-use of its solutions including by those interested Member States, companies and Research and Technology Organisations (RTOs) that will not be participating in the IPCEI-CIS.

The pre-notified IPCEI-CIS aims at developing and industrially deploying, for the first time, a fundamentally new, innovative, secure and sustainable data processing production process spanning across the European Union. It will develop and deploy breakthrough technological cloud and edge computing capabilities and very high added value data processing industrial services.

Member States envisage to support the IPCEI-CIS with State aid and to this end will notify their individual projects under the IPCEI State-Aid Communication to the Europeans Commission's Directorate General of Competition. The IPCEI Exploitation Office will not interfere with the individual responsibility of the Member States or companies to implement the Commission decision on the IPCEI-CIS but will regularly report on and monitor the progress set out in the Commission's decision on State-aid.

The pre-notified IPCEI-CIS will contribute to existing European initiatives, in particular to the European Green Deal, the European Industrial Strategy, the Digital Compass and directly to the implementation of the High Impact Project of the European Strategy for Data.

Scope:
This action consists in providing at least the following core strategic and support activities via the set-up of a Cloud IPCEI Exploitation Office that will maximize the benefits and exploitation of the developed IPCEI solutions towards all interested Member States, companies and RTOs: Management and Operations Activities: Monitoring and reporting. This should include: (i) the IPCEI project deliverables - including the new solutions developed and industrially deployed - their impacts and timing, (ii)

the key performance indicators associated to each of the IPCEI-CIS project spill-over activities; (iii) the sustainability performance and security features of the integrated IPCEI project and; (iv) macro-project outcomes (Macro-projects under the IPCEI-CIS aim to provide a deeper level of European integration to commonly achieve the objectives of the integrated project, by delivering common results, products or services).Where necessary, risk mitigation activities to guarantee effective and timely delivery and reuse of all the IPCEI-CIS project deliverables.The necessary ICT tools for the functioning and use of the pre-notified IPCEI-CIS activities and solutions, notably to (i) allow both IPCEI participants and non-participants to secure and effectively collaborate and; (ii) ensure external communication activities.Support the applications process and alignment of the assessment process of potential new participants. Sustainability Activities: Support the development of the medium-term sustainability strategy, governance and decision-making process of the pre-notified IPCEI in close collaboration with the governmental Authorities participating in the IPCEI-CIS and the European Commission.Develop joint approaches to ensure that project results stemming from the IPCEI-CIS (such as open-source software technologies) will be maintained and regularly updated. Dissemination and Exploitation Activities: Support the pre-notified IPCEI-CIS main dissemination and exploitation activities to reach scale beyond the IPCEI participants including in preparatory activities, organization, logistics and content materials for each of its key events and meetings.Foster transparency of the pre-notified IPCEI-CIS activities and wide uptake of the new innovative cloud-to-edge solutions to be first industrially deployed by for example preparing IPCEI-CIS communication materials, including social media content, to regularly and at large scale communicate about the status and content of the IPCEI-CIS activities, projects and new deployed solutions that all interested stakeholders have regular access to up to data information.
The consortium could be structured around public or/and private organisations, used to conduct complex and large coordination and management work with public authorities and private organisations, to monitoring of technical deployments (notably security and sustainability aspects), and that are capable to demonstrate a good technical and policy understanding of the domain at European level.

2. DIGITAL-2023-CLOUD-AI-04-GENOME (DIGITAL-SIMPLE)

Genome of Europe

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SIMPLE DIGITAL Simple Grants	

Expected Outcome:
Joint or coordinated sequencing (WGS), as described under Scope.New WGS data for a large number of representative European citizens, to be further specified in the call document, generated in accordance with the guidance, specifications and standards agreed within 1+MG (1+MG Trust Framework).Integration of eligible population-based WGS data generated independently of the GoE and made available to the project.The Genome of Europe federated reference database established and accessible through the federated European genomic data infrastructure and the European Health Data Space (EHDS) infrastructure for secondary use of health data (HealthData@EU).

Objective:
This action will support the implementation of the Genome of Europe (GoE) multi-country project and contribute to achieving the objectives and long-term ambition of the 1+Million Genomes (1+MG) initiative. GoE aims to establish and launch a European reference genome database of genetic variation obtained by whole genome sequencing (WGS) for at least 500,000 citizens based on population-based national reference genome collections, collectively representative of the European population. GoE has the potential to foster break-through advances in research, innovation, disease prevention and healthcare delivery, widely spread across clinical disciplines, beyond current use cases (disease areas). Moreover, creation of a reference database will allow meaningful savings in healthcare systems as it will enable data imputation and enrichment of genotype information. A concerted genome sequencing effort is necessary to achieve a critical mass of WGS data across Europe. By fostering it, this action is expected to bring major efficiencies due to economies of scale and should enable all GoE countries to contribute with WGS data. It will also ensure consistent application of agreed common data requirements and quality measures across all national datasets, enabling the creation of a high-value European reference dataset.

The objective is also to support the initiative taking into account the potential creation of a European Digital Infrastructure Consortium (EDIC).

Scope:
The focus of the action is on whole genome sequencing at clinical grade depth necessary for clinical application. This can be achieved by coordinated WGS sequencing expected to enable massive new data collection in all GoE countries. WGS data for the GoE must be generated following the 1+MG Trust Framework that brings together a set of minimal recommendations to enable secure cross-border access to genomic data in Europe, in particular as regards ethical and legal aspects, data standards, data quality and technical inter-operability. To this end, sequencing specifications should follow the available 1+MG guidance and align closely with that initiative.

The biological samples needed to generate the data, i.e., to sequence the genomes, can either originate from existing population-based cohorts and national biobanks, or be collected from participants recruited specifically for the national and European GoE reference databases. The participants will be selected at the national level to be representative of the respective population, including a contribution of relevant minorities. To ensure uniform approach, the exact inclusion and selection principles need to be agreed at the European GoE level.

In parallel to data generating activities (WGS sequencing), the architecture, hardware and software necessary to aggregate national reference databases into a European reference database (The Genome of Europe) need to be designed, developed and implemented in cooperation with the Genomic Data Infrastructure (GDI) project. As well as newly generated GoE data, this

should ensure effective integration of available national population-based WGS collections established before or independently of the GoE. The GoE database must be interoperable with and accessible through the 1+MG data infrastructure and equally aligned with the European Health Data Space (EHDS), in particular the infrastructure for secondary use of health data (HealthData@EU).

For data security reasons, sample transport, all WGS activities and genomic data transfer and storage must take place within the territory of eligible countries.

The GoE project forms an integral part of 1+MG and GoE data will be accessible via the European federated genomics data infrastructure (GDI) deployed under the Digital Europe topic DIGITAL-2021-CLOUD-AI-01-FEI-DS-GENOMICS. Besides Digital Europe's Data Spaces, the topic is also synergetic with the RRF support for the GoE multi-country project as stipulated in the national recovery and resilience plans of several Member States. Cooperation with other relevant European initiatives, and due consideration of other projects and infrastructures, for example those funded under the Horizon 2020 and Horizon Europe research and innovation programmes and the EU4Health Programme (e.g. Genomics for Public Health), will be strongly recommended to build on and bring forward their results as well as to ensure a good use of synergies and complementarities.

The awarded project will use, in so far as possible, the smart cloud-to-edge middleware platform Simpl, and have to work in partnership with the Data Spaces Support Centre deployed under the first W in order to ensure alignment with the rest of the ecosystem of data spaces implemented with the support of Digital Europe Programme. The joint work will target the definition of the data space reference architecture, building blocks and common toolboxes;the common standards, including semantic standards and interoperability protocols, both domain-specific and crosscutting;
The data governance models, business models and strategies for running data spaces.

3. DIGITAL-2023-CLOUD-AI-04-DEVELOPCITI (DIGITAL-SIMPLE)

Developing citiverse

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SIMPLE DIGITAL Simple Grants	

ExpectedOutcome:
The action will result in one or more projects proposing varied use cases for the CitiVerse. Such project(s) may be focusing on the same pilot areas envisaged by the EU Smart Communities data space project (call 3 [DIGITAL-2022-CLOUD-AI-03-DS-SMART]), although focus on other pilot areas is also possible. The concept could also be built on the existing EU data infrastructure and interconnected Local Digital Twins.

The project(s) should also propose a roadmap to expand CitiVerse solutions in Europe using Minimal Interoperability Mechanisms (MIM)-compliant standards and EU technology solutions and make recommendations for interoperable and open CitiVerse platforms in line with EU values and policy landscape.

Objective:
The action will help define what the 'CitiVerse' means for Europe building on the smart communities' data infrastructure that is developed under WP2021-22 and WP23-24. The objective is to bring EU CitiVerse industry, including SMEs, together in developing the different layers of VR/AR worlds useful for local authorities and citizens. The project(s) stemming from this action will take into account potential EDIC in the field.

The action could build on existing local digital twins expanding their capabilities. One or more projects, led by the industry in cooperation with one or more communities, will introduce VR/AR and metaverse technology to allow citizens and other stakeholders to «navigate and interact» in their urban spaces from basic 'default' sensory experiences all the way to digital asset-enhanced AR overlays merging the physical and virtual communities into a hybrid metropolis. This will create a steady and immersive environment for citizens and businesses, a CitiVerse, that can be used for virtual/real spatial planning, management or navigation while also enhancing the social, architectural, green and cultural heritage dimension of living spaces.

Use cases will span from hybrid systems to fully-fledged verses created with data coming from various data sources, notably from the EU data spaces such as the smart cities and communities, but also from other public and private sources. European industry, including the wealth of European SMEs active in technologies relevant for metaverses and in content creation, will contribute to its development, taking the leadership in an area rich of possibilities. The action will contribute to the ecosystem of SMEs and larger companies nurtured through the VR/AR Industrial Coalition, and at the same time it can benefit from the mobilising and structuring actions of the Coalition as well as from integrating the values and principles of the New European Bauhaus initiative. The action should also explore links and synergies with the Climate-neutral and smart cities Mission, and in particular to selected Mission cities, when identifying use cases.

Scope:
In particular, the action will:
Start developing the CitiVerse for citizens to offer them interoperable and sustainable services. Develop concrete CitiVerse use cases (and combinations of them) in the area of navigating in a community, discovering its assets such as culture, history, tourism and offering innovative services related to tourism, entertainment, shopping, future development and urban planning, etc., infrastructure management and sustainable mobility.Encourage EU technology providers to integrate various data sources together to develop and train AI in a new specific CitiVerse context. Activate a network of EU industrial partners, including SMEs, in Member States to provide technology capacity for the CitiVerse. This network may be part of, and interact with, the VR/AR Industrial Coalition and/or the New European Bauhaus initiative. Identify building visualization solutions and multi-dimensional

models to implement CitiVerse prototypes. Exploit the long tradition of Europe in cultural and media content, involving European content creators, in particular SMEs, in the design of engaging in immersive CitiVerse environments. Work towards recommendations for a robust, open and interoperable CitiVerse legal framework compatible with EU values and laws. Include security by design and plan how CitiVerse applications and platforms can be used in real-life contexts.

4. DIGITAL-2023-CLOUD-AI-04-AEROSEC (DIGITAL-SIMPLE)

Highly secure collaborative platform for aeronautics and security industry

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SIMPLE DIGITAL Simple Grants	

ExpectedOutcome:
A commercially viable highly-secure cloud-based collaborative platform for the management of industrial programmes in the aeronautics and security sector.The governance implications that the operations of such a platform would have on the sector, notably how such platform can operate, be deployed, be accessed, and how projects can be managed through their lifecycle.A significant contribution to the discussions for an EU-level single set of rules and accreditation for data sharing in the aeronautic and security sector.

Objective:
The objective is to develop a commercially viable highly secure cloud-based collaborative platform for the management of sensitive multi-country industrial initiatives in the aeronautics and security sector, including civil security.

This platform will allow the development of highly sensitive industrial projects, from design to production. In particular, the platform should be able to support the development of products and services financed under future calls of the European Defence Fund.

The need for a new platform derives from the very specific requirements from the aeronautics and security sector. Over the years, the European industry in general has embraced several paradigm changes resulting from new ICT capabilities: collaborative platforms, co-design, concurrent engineering, decentralised and multi-supplier collaboration, the virtualisation of software and hardware, etc. But the aeronautics and security sector has only embraced such changes with caution, if at all. This is due inter alia to different national standards for the classification of data, complex user-access requirements or justified localisation obligations for data infrastructures, typically on the grounds of public security. Such situation has become untenable and seriously undermines the sector's competitiveness against other world's regions, not the least against an international context that implies the multiplication of multi-country and multi-stakeholders' projects.

Scope:
The highly secure collaborative platform should:
Allow the aeronautics and security sector to reach a similar level of decentralised/distributed working along its supply chains as other sectors already enjoy today (e.g. the automotive sector).Be cloud-based (i.e. operated from a highly-secure cloud infrastructure), as opposed to require on-premise software deployment.Provide for a broad range of secure and user-friendly collaborative tools including general purpose collaboration tools (messaging, wikis, file sharing, videoconferencing, chat) as well as more advanced tools (computer-assisted design, product lifecycle management, data analysis…).Provide for a stack as deep as needed to cater for the specificities of the aeronautics and security sector, including where applicable at IaaS and PaaS levels.Cater for state-of-the-art security, interoperability, reversibility, sovereignty and sustainability standards.Allow for the concurrent management of different industrial programmes without the need to duplicate the platform (for each programme/country/contractor/etc).Be anchored in the security requirements specific to the aeronautics and security sector.Cater at minima for the specific needs of information classified at the level of RESTRICTED and equivalents (cf. equivalence table in Council Decision 2013/488/EU and Commission Decision (EU, Euratom) 2015/444), and allow ad-hoc segregation to handle specific national needs or requirements. To the extent possible, the collaborative platform should provide sufficient safeguards so that physical segregation of data is no longer required.Incorporate, where appropriate, the outcome of a possible process for defining an EU-level single set of rules and accreditation for data sharing in the aeronautic and security sector.Allow for the evolution over-time of the platform, given the very long industrial cycles specific to the aeronautic and security sector

(50+ years).Allow for multi-cloud tenancy.Be tested in quasi-real situations, for example by using it in a real co-design situation which, in reality, does not imply particular confidentiality but where hard user access controls are simulated.
The following items fall outside of the scope:
the provision of the hardware infrastructure to deploy and operate the platform
The consortium should be structured around private stakeholders (typically: software vendor, data infrastructure providers, aeronautic and security stakeholders, cybersecurity stakeholders). However, to maximise its impact, public authorities, in particular Ministries responsible for national security, home affairs and/or defence, should as well integrate the consortium. Higher education entities, and research and technology organisations with demonstrated cooperation with the above-mentioned public/private stakeholders could also join the consortium where they can make a distinct contribution to the development of the envisaged platform.

5. DIGITAL-2023-CLOUD-AI-04-COORDINATEF (DIGITAL-CSA)

Coordination of AI sectorial testing and experimentation facilities

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-CSA DIGITAL Coordination and Support Actions	

Expected Outcome:

Action plan organised along different domains: technological, business models, skills development, dissemination, legal aspects, outreach, etc., to develop links and synergies with EDIHs, data spaces, edge AI TEF, network of AI research excellence centres, and the AI-on-demand platform.A catalogue of common resources and services across the TEFs.Joint dissemination and communication plan with TEFs on their activities and services, to be implemented within the project duration.A specialised support unit to coordinate co-funding instruments, including regular interactions with Member State's administrations, including with regards to Grant Agreements.Technical mechanisms for a seamless exchange of assets with the AI-on-Demand platform. Delivery of individual and targeted sectorial sections within the platform (distributed model).A specialised business consultancy unit focussing on business and go-to-market strategy, optimising TEF business sustainability.Periodic impact assessment and road-mapping: collection and analysis of the key performance indicators (KPI) defined for the TEFs and sharing of good practices and lessons learnt.

Objective:
The Coordination and support action grant will support the sectorial Testing and Experimentation Facilities (TEFs) created under the WP 2021-2022 (Health, Manufacturing, Agri-Food, Smart Cities and Communities) and the future new ones to be create under the Digital Europe Programme, to develop complementary cross-TEF activities in providing AI services from a cross-sector perspective, to maximise the overall impact of TEFs in their ambitions of achieving world-class excellence and help the sectorial TEFs to better link with relevant EU projects, initiatives and stakeholders in the AI ecosystem of excellence. By boosting the reinforcing feedback loops, the CSA will also bolster the sectorial TEF's and the ecosystem's sustainability.

Once the sectorial TEFs funded under the 2021 call are established, it is necessary to coordinate the TEFs with other actions launched in the Digital Europe Programme (in particular data spaces, the edge AI TEF, the AI-on-demand platform, relevant cloud and HPC initiatives) and to develop a strong ecosystem around the TEFs enabling a faster and growing adoption of AI technologies in the European market.

Scope:
The CSA will help develop synergies and exchanges between the TEFs, and with other relevant projects, such as the European Digital Innovation Hubs (EDIHs), data spaces, network of excellence research centres, and other actions funded e.g. under DEP and Horizon Europe, AI-on-demand platform, and the community at large.It will establish strong links with Edge to Cloud and relevant HPC actions funded under strategic objective 1 (EuroHPC JU), using when appropriate the SIMPL platform as a connector, and help TEFs to make the most out of all these resources and services.It will support the running projects in allowing economies of scales regarding common activities run by the individual networks (e.g., organization of events, access to common resources, mentoring and exchange mechanisms among TEFs, integration with 3rd party services and other EU funded projects, etc.) and exchanges of best practices to reinforce and optimize cooperation.It will support TEFs to help companies using their services to comply with the AI Act. This could be through regulatory sandboxes, standards, certifications, labelling schemes, research methodologies for the explainability of AI systems and collaboration with public authorities, depending on what TEF themselves offer and what additional or complementary support to the companies is needed.It will support TEFs in their dissemination activities towards industry, users and public administrations. Special attention should be on coordinating mentoring and twinning programmes for innovators in order to foster fair participation and potential expansion of TEFs activities

across Europe to complement and reinforce the on-going TEFs. It should contribute to the visibility of AI & robotics in Europe, building on technologies tested in TEFs and targeting sectorial audiences, with a clear focus on real world applicability.Support and coordination with regards to co-funding instruments, helping TEFs in common approaches towards Member States including support and exchange of best practices in the implementation and reporting requirements imposed by state-aid rules, contractual requirements, interpretation of the Grant Agreements etc.Act as facilitator for cooperation with the AI-on-demand platform. Foster contribution from TEFs and channelling TEFs needs towards the AI-on-demand platform.Facilitate coordination with the edge AI TEF. Solutions developed and tested in the former could be later integrated and tested in the sectorial TEFs.The CSA will establish the necessary resources to help and support TEFs in their coordinated go-to-market approach, including but not limited to sustainability plans, sale strategies, price lists, etc.Facilitate exchanges with EDIHs and national competence centres, etc. to maximise the opportunities offered e.g., to maximise the outreach to all regions across Europe).Support the European Commission in the monitoring of existing TEFs, assessing progress and providing recommendations for their implementation and drawing lessons for policy-making.Targeted stakeholders: The consortium should include a relevant representation of all the sectorial TEFs selected from the 1st call of the Digital Europe Programme, to ensure that the selected CSA optimally support their coordination. These organisations will be subject to Article 12(6) of Regulation (EU) 2021/694.

6. DIGITAL-2023-CLOUD-AI-04-ICU-DATA (DIGITAL-SIMPLE)

Federated European Infrastructure for intensive care units' (ICU) data

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SIMPLE DIGITAL Simple Grants	

Expected Outcome:
Deployment of an interoperable and secure federated infrastructure for trusted ICU datasets in the EU, and linked to AI resources, with established interoperable links to other federated European data infrastructures, such as on cancer-imaging and genomics.Secure and interoperable platform for aggregation of ICU datasets for secondary analysis and development of toolsets on relevant datasets for different treatment types useful for developing clinically relevant AI algorithms for specific use cases, including test and training data sets (“atlas” of anonymized Acute Care cases);Computational modelling tools for individual ICU patient patho-physiology simulation and analysis using ICU related clinical information (including decision-support tools), clinical consultation, collaboration and monitoring, that are fully interoperable.Platform and mechanisms to exchange best clinical practice and adapted analysis and training datasets, also in case of an emerging health threat event, such as a pandemic.User Interface front-end module or system at the workforce level operational in minimum four EU languages. Design development in co-creation with the workforce with demonstrated improvement of provision of care: processes, documentation, quality control including new, adapted or extended ICU data sources including annotation, voice recognition, integrated datasets.A sustainable operational coordination and governance structure, open to the involvement of new stakeholders, including capacity building measures necessary to ensure the establishment, sustainable operation and successful uptake of the infrastructure with the ultimate aim to establish an entity under European law.A business model including an uptake strategy explaining the motivation and incentives for all stakeholders at the different levels (regional, national, European, global) to support the data infrastructure towards its sustainability, including data controllers, data users, service providers, healthcare workforce, systems and public authorities at large and taking into account the role of SMEs in the deployment and the value chain;A training and skills programme supporting the interdisciplinary nature of the subject matter and enabling the sustainable development, integration and use with a strong view to innovation, provision of citizen-centred health and a better quality of life for citizens and society.

Objective:
The action will establish and deploy a pan-European federated infrastructure for Intensive Care Units’ (ICU) data combined with governance mechanisms allowing secure cross-border access to ICU datasets. The infrastructure shall primarily address data from acute care, including data generated from physiological monitors, laboratory investigations, imaging, clinical examination and examination protocols, and therapeutics as well as from emerging omics technologies used during the delivery of care. It shall be used by clinicians, researchers and innovators with the ultimate aim of more precise, faster and more effective clinical decision-making, diagnostics, treatments and predictive medicine. This infrastructure shall allow for both observational and interventional research and innovation to occur at pan-European level, also in preparation for possible future pandemics.

The ICU data infrastructure shall be supported by advanced corresponding IT tools and capacities in terms of data capture, processing, analysis and visualisation, with inherent interoperability and connectivity, enabling secure access to and distributed analysis of datasets, including AI use. In addition, it should support the exchange of best practices with a fast-track approach for addressing emerging need, such as in case of a pandemic. Finally, it shall be supported by a corresponding package for digital skills training and education as fit for the purpose for this scope.

Scope:
The awarded action will support the deployment of the infrastructure needed to link and explore fragmented European

databases of Intensive Care Units on acute care and telemedicine, complemented by a solid governance and a clear and sustainable business model for gathering data, models and best practice, and its exploitation by public and private organisations towards clear benefits for health communities and society. It will provide a harmonised approach for accessing acute care-related data and linking it with other health data sources enabling data discovery and re-use for researchers, innovators, clinicians, as well as AI and data tool developers. The action should contribute to supporting decision-making and improving patient care in the ICUs, through better short-term prediction and earlier identification of critical clinical status of patients, including for infectious diseases. It will also facilitate chronic and inherent risk factor identification, including for cancer. The action shall also establish a basis for data intensive computational model-based tools for decision support and risk prevention, towards a "virtual twin of an ICU patient".

The action shall address the interoperability requirements so that communication and exchange of data and information within and between ICUs is fully enabled. The proposal shall identify flexible common data models, core sets of standardized data elements and anonymisation strategies, and be in full compliance with the principles of GDPR, patient privacy, as well as accordance with the FAIR principles. The work shall be based on common data models, interoperability mechanisms, intra- and inter-EU national collaborative exchange of data and knowledge including teleconsultations and synoptic near real-time sharing of clinical data to account for the urgency to treat within this medical discipline. The action shall set up a federated infrastructure of ICU data in Europe which would facilitate the development of short-term predictive models, better decision support tools and model (incl. AI) -based risk prevention tools helping intensivists in their work.

The action is expected to engage with ICU centres and relevant stakeholders in all EU Member States and regions with a view to increasing the representativeness of the ICU data sources vis-à-vis the European population, types of diseases covered, and sufficient quantity and quality of data for research and innovation. The action shall promote the effective implementation and evaluation of data-driven systems in Intensive Care. Implementation should be ICU practitioner-centred and designed according to the needs of users, notably the health workforce providing the care in practical terms and taking into account continuity of care. Incentives for use must be considered and added value demonstrated in terms of process facilitation or innovation and better outcomes.

The resulting data infrastructure should be aligned with the developments under the European Health Data Space (EHDS). It should be inter-operable with other building blocks and components of the EHDS, and the federated European infrastructures for genomics data and for cancer imaging data. The work should build on and bring forward the results accomplished in relevant Horizon 2020 and Horizon Europe projects and the Digital Europe Programme. It shall engage and coordinate with the relevant actions of the health cluster of the Digitizing European Industries (DEI) initiative, the European Reference Networks and the ongoing cooperation of ICU Hubs between Member States and regions with a view to establishing and fostering interoperability, harmonisation and standardisation.

The awarded project(s) will use, in so far as possible, the smart cloud-to-edge middleware platform Simpl, and have to work in partnership with the Data Spaces Support Centre deployed under the first WP in order to ensure alignment with the rest of the ecosystem of data spaces implemented with the support of Digital Europe Programme. The joint work will target the definition of the data space reference architecture, building blocks and common toolboxes to be used;the common standards, including semantic standards and interoperability protocols, both domain-specific and cross-cutting;
The data governance models, business models and strategies for running data spaces.

7. DIGITAL-2023-CLOUD-DATA-04-DIGIPASS (DIGITAL-SIMPLE)

Digital Product Passport

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SIMPLE DIGITAL Simple Grants	

Expected Outcome:
Deployed and validated at scale and real life setting Digital Product Passports in at least two value chains.Report on further needs for standardisation and specifications to ensure interoperability, security and acceptance by all the stakeholders.Recommendations based on the lessons learnt for the deployments of DPP in other value chains.

Objective:
To enable sharing of key product related information that are essential for products' sustainability and circularity, including those specified in Annex III of ESPR proposal, across all the relevant economic actors. Consequently, to accelerate the transition to circular economy, boosting material and energy efficiency, extending products lifetimes and optimizing products design, manufacturing, use and end of life handling.To provide new business opportunities to economic actors through circular value retention and optimisation (for example product-as-a-service activities, improved repair, servicing, remanufacturing, and recycling) based on improved access to data;To help consumers in making sustainable choices; andTo allow authorities to verify compliance with legal obligations.

Scope:
Support one Pilot action that will demonstrate in real setting and at scale DPPs in at least 2 value chains (product categories) with a preference to those with long and complex supply chain and/or challenging repair, refurbishment and recycling. This DPP information system should rely on international or European standards in the following areas: data carriers and unique identifiers, access rights management, Interoperability (technical, semantic, organisation) including data exchange protocols and formats, data storage, data processing (introduction, modification, update), data authentication, reliability, and integrity, data security and privacy. Where possible, this will consist in using the smart cloud-to-edge middleware platform Simpl. The access to information included in the DPP should be role-dependent (i.e., differentiated by stakeholder type). The full interoperability of the same DPP information system among different supply chains should be one of the characteristics tested and proven by the pilot.

The pilot will build on the available results of the Coordination and support action (CIRPASS)as well as other relevant initiatives. It will also consider the appropriateness of the latest tracking and tracing technologies, internet of things systems, distributed ledger technologies, cybersecurity methods and cloud technologies and infrastructures (such as GAIA-X).

A specific contribution is expected on demonstrating at large scale the feasibility of acquiring, managing and securely sharing the data held or generated by operators such as supply chain actors, manufacturers, resellers, repairers, remanufacturers, and recyclers, along these value chains for which an access by other relevant stakeholders would have a major beneficial impact on circularity and sustainability.

The real-life deployment should validate and further improve protocols for secure and tailored access for the relevant stakeholders. It should test in real life setting open digital solutions for identification, tracking, mapping and sharing of product information along its life-cycle, ensuring interoperability across borders and a well-functioning EU Internal Market. This pilot will build on existing open international and European standards with the aim to provide for a consistent operational framework.

8. DIGITAL-2023-DEPLOY-04-EDMO-HUBS (DIGITAL-SME)

European Digital Media observatory (EDMO) - National and multinational hubs

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SME Digital SME Support Actions	

Expected Outcome:

At the end of the actions, a network of existing and newly established research hubs will be active across the EU under the coordination of EDMO.Networks of experts and organisations linked to the hubs will be part of a European multidisciplinary community which will actively detect, analyse and expose disinformation campaigns in Europe.Each hub will have produced or contribute to at least 100 fact-checks, 20 investigations and reports on disinformation campaigns and shared them through EDMO.Each hub will have established at least 10 tailor-made media literacy programs in Member States and produced reports (at least 1 per year) regarding the implementation and effectiveness of online platforms policies to tackle disinformation.

Objective:
The European Digital Media Observatory (EDMO) has been created with the aim of supporting an independent multidisciplinary community to tackle the phenomenon of disinformation. EDMO is composed of a central platform and governance which support and coordinate the work of the EDMO national/multinational hubs.

The objective of this topic is to finance the work of independent national /multinational hubs for analysis of digital media ecosystems in order to ensure the coverage of geographical areas covered by the EDMO hubs for which the funding is ending at the end of 2023 and in 2024.

A national/multinational hub involves organisations active in one or several Member State(s), that will provide specific knowledge of local information environments so as to strengthen the detection and analysis of disinformation campaigns, improve public awareness, and design effective responses relevant for national audiences. The activities of the hubs should be independent from any public authority.

These national/multinational centres will focus their activities on emerging digital media vulnerabilities and disinformation campaigns, which are of special relevance within the territory and/or linguistic area in which they will operate. Multinational hubs will cover more than one Member State with similar media ecosystems within an EU region.

Scope:
Support will be provided to:
Support the operations of an independent national or multinational hubs pulling together a national/multinational multidisciplinary community composed of academic researchers, fact-checkers, open-source investigation organisations, media practitioners and other relevant stakeholders in order to create a network capable of quickly detecting and analysing disinformation campaigns, as well as producing content to support national and local media and inform about regarding emerging harmful disinformation campaigns. They will work in cooperation with EDMO and contribute to its activities providing fact-checks, media literacy materials, scientific articles, surveys on disinformation trends, situational analyses and assessments of online platforms' policies to address disinformation-related harms.Detect, analyse, and disclose disinformation campaigns at national, multinational and EU level, and their impact on society and democracy. To this end hubs will analyse relevant actors, vectors, tools, methods, dissemination dynamics, and targets of disinformation campaigns in coordination with EDMO. Hubs will monitor the evolution of disinformation-related harms on relevant audiences. Each hub will also support a regular assessment of the impact of relevant disinformation campaigns on society and democratic processes, as well as the effectiveness of the policies

set out by online platforms to counter various disinformation phenomena. In addition, the hubs will actively participate to the EDMO joint activities of fact-checking and research and promptly react to EDMO requests linked to emerging disinformation issues.Create tailor-made media literacy campaigns for the covered territory or linguistic area. Hubs will leverage on the exchange of good practices and materials coordinated by EDMO and contribute to the EDMO repositories with newly created educational and training materials.Cooperate with national authorities for the monitoring of online platforms' policies and digital media ecosystem in the territory or linguistic area covered by the proposal. In particular, they will provide relevant insights which might help competent national authorities, including the audio-visual regulator(s), monitoring the implementation of the Strengthened Code of Practice on Disinformation by its signatories.

9. DIGITAL-2023-DEPLOY-04-NETWORK-OF-SICs (DIGITAL-SIMPLE)

Network of safer Internet Centres (SICs)

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SIMPLE DIGITAL Simple Grants	

Expected Outcome:

National SICs as a one-stop-shop for reliable and age-appropriate information.Digital literacy in Member States and associated countries in formal and informal education settings (e.g., youth participation activities, workshops, classroom visits, competitions, peer to peer activities).Support to parents, carers, teachers, educators and other professionals working with children to better understand the risks and opportunities of children accessing digital content and services (e.g., information sessions, train the trainers programmes, and online and offline material).Timely information to local, national, and European actors on emerging risks through the helpline service.Access to resources and services by public authorities, including law enforcement agencies, and exchanges with hotline analysts to develop better preventive measures and to remove online child sexual abuse material (CSAM).Increased cooperation of the private sector with the SICs, including those recognised in the future as "trusted flaggers" to assist the public, in particular children, when confronted with harmful and illegal content.

Objective:

The objective of the topic is to continue to support national SICs which may be composed of one or more NGOs, government bodies/agencies, private sector organisations in providing online safety information, educational resources, public awareness tools and counselling and reporting services (through dedicated helplines and hotlines) for young people, teachers, and parents. The activities performed by the SICs will help minors to tackle online risks and to become media-literate, resilient, digital citizens, and will allow citizens to anonymously report online child sexual abuse material (CSAM).

To reach all children, the Safer Internet Centres will pay particular attention to children with special or specific needs, including those from disadvantaged and vulnerable backgrounds.

Scope:

The funding will ensure the continuation of the well-established European network of national SICs, by enabling the awarded consortia to provide at least:

A centre for raising awareness among children, parents/carers, teachers and educators as well as other relevant professionals working with children about online opportunities and risks for the under 18s. The focus will be to identify and address: specific and general emerging risks (e.g. new apps and games, but also AI, virtual, augmented and extended reality, the internet of things and other technological changes raising new social and ethical challenges that impact children); issues such as mental and physical health risks related to the use of technologies (e.g. self-harm, cyberbullying, risky online challenges, promotion of eating disorders); risks facing children as young consumers (e.g. nudges to spend money, aggressive marketing strategies, lootboxes) on which specific attention will be paid. A helpline to give advice and support to parents and children on issues related to children's use of digital technologies and services; to strengthen support to victims of cyberbullying, closer cooperation with the national Child Helpline 116111 service is required.A hotline for tackling CSAM (i.e., receiving, analysing, and processing reports of such material). Closer cooperation with law enforcement and the private sector should be further explored in the context of the EU strategy for a more effective fight against child sexual abuse and the proposed new legislation.A youth panel to engage directly with children from different demographic groups, including the organisation of regular youth participation activities, allowing them to express their views and pool their knowledge and experience of using online technologies. Adequate turnover and an open selection of participants is required.

SICs shall strengthen their support to children in vulnerable situations (such as children with disabilities, children from a minority, racial or ethnic background, refugee children, children in care, LGBTQI+ children, as well as children from a disadvantaged socio-

economic background, who all may face additional challenges in the digital environment). For example, to address the digital divide, they should offer non-formal education and training to these groups and communities.

In addition, SICs will:
support the monitoring of the impact of the digital transformation on children's well-being in cooperation with the BIK platform,support the implementation of relevant EU strategies,promote the distribution of relevant online training modules (MOOCs) for teachers,expand the role of BIK Youth Ambassadors and BIK Youth Panels to support peer-to-peer activities at national, regional and local level,provide trustworthy resources for and carry out campaigns targeting children, parents, carers and teachers, educators and other relevant contacts working with children (e.g. sports coaches, club leaders). Training on children's rights online should also be included in these initiatives to create a stronger awareness that children's rights online are the same as offline, as stipulated by UN General Comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25).

10. DIGITAL-2023-DEPLOY-BESTUSE-TECH-04-ENERSAVING (DIGITAL-SIMPLE)

EU Energy saving reference framework

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SIMPLE DIGITAL Simple Grants	

Expected Outcome:
An EU Energy saving Reference Framework that should lead to a standardised reference application that will be developed in close collaboration with energy providers and will draw from applications and services already available in the market. The deployment of the EU Energy saving Reference Framework across the Union in close collaboration with energy providers.

Objective:
The current context – Russia's invasion of Ukraine and the accompanying high inflation – compels us to accelerate the energy transition and save energy to ensure a sustainable, resilient, and fair economy. This entails making better use of the data that is generated all along the energy supply chain and to exploit the potential of digital technologies to reduce demand, eliminate wastage and reduce energy bills.

Smart meters and smart apps enable consumers to reduce and optimise their energy consumption and cut their energy bills. They provide greater consumer awareness and opportunities to monitor and control in real time the energy consumption of their appliances. Across the European Union, however, the functionality and availability of such meters and apps remain very fragmented.

The Digitalisation of Energy Action Plan adopted on 18 October 2022, sets out for the European Commission, working with Member States, to develop a common European reference framework, including an open-source reference implementation, for a consumer application that allows for voluntary reductions in energy consumption and thereby help reduce energy costs.

Scope:
The scope of this action is to develop and deploy an EU Energy saving Reference Framework as a key tool to conserve electricity when there is an anticipated shortage of energy supply. Alerts are to be based on energy generation data and real time energy consumption. Clear messages are to guide consumers to adopt the right measures to ensure a good energy supply for all. For example, following an alert, consumers can voluntarily reduce their electricity consumption and thereby contribute to avoiding possible power blackouts.

11. DIGITAL-2023-PROGRAM-SUPPORT-04-DISSEM-EXPLOIT (DIGITAL-CSA)

Support to Dissemination and exploitation (D&E)

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-CSA DIGITAL Coordination and Support Actions	

ExpectedOutcome:
A conceptual and operational framework for D&E taking into account the elements mentioned under “scope” and offering solid methodological and practical approaches. A proposal for a set of actions to be implemented by the different stakeholders and a plan to deliver on the framework, with monitoring and evaluation metrics. The implementation of relevant actions aiming at e.g. supporting and complementing individual projects efforts in their D&E activities. The analysis of possible means and tools to support the delivery of the framework, including a proposal for the functionalities of the Digital Europe Programme Results Platform (see the Digital Europe Programme Model Grant Agreement Art. 17 and its Annex 5) in the light of the Horizon Europe Results Platform.

Objective:
The action will maximise the impact of the Digital Europe Programme and the take up of its results through a Dissemination and Exploitation (D&E) conceptual and operational framework, including the delivery of a number of practical actions.

Scope:
The action will address at least the following dimensions:
the overall programme, its Specific Objectives (SO) and areas therein, down to topics and projects where appropriate; the capacity building and use strands of Digital Europe Programme; the different stakeholders; the stages of the project lifecycle and the reporting obligations;coordination within EU and beyond when relevant, taking into account the policy priorities and initiatives; between projects of Digital Europe Programmes and other programmes (e.g. Horizon Europe);within Digital Europe Programme itself, identifying and exploiting complementarities of projects among SO and topics;between Digital Europe Programme and EU member states national/regional programmes; of the different programme implementing bodies, e.g. European Commission, Health and Digital Executive Agency (HaDEA), JU and similar bodies.
The action will consider means that can help delivering its objective, including the pertinence of leveraging already existing tools, e.g. of other EU programmes like Horizon Europe. The action will consider innovative approaches to D&E and how to improve the uptake of Digital Europe Programme results beyond the entities directly involved in the projects.

12. DIGITAL-2023-PROGRAM-SUPPORT-04-NETWORK-NCPs (DIGITAL-CSA)

Supporting the network of National contact points (NCPs)

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-CSA DIGITAL Coordination and Support Actions	

Expected Outcome:
The action is expected to contribute to the following outcomes:
Improved and professionalised NCP services across Europe, supporting access to Digital Europe Programme calls, lowering the entry barriers for newcomers, and raising the average quality of proposals submitted;Robust NCP support services across Europe that are adapted to specific objectives of Digital Europe Programme, including; more participation of new players in the programme;matchmaking activities to connect potential participants from widening countries with emerging consortia in this thematic area using a variety of tools;dissemination of information about security and ownership control rules in Digital Europe Programme for applicants.

Objective:
This action will support the coordination between different National Contact Points (NCPs) for the Digital Europe Programme, the preparation and execution of actions that maximise awareness and the impact of the programme and the long-term dissemination and exploitation of results.

The selected project will provide support for all specific objectives of Digital Europe Programme.

Scope:
Proposals will contribute to the development of a specific NCPs network for Digital Europe Programme.

Proposals should facilitate trans-national co-operation amongst NCPs, encouraging cross-border activities, sharing good practices and raising the general standard of support to programme applicants and facilitate participation of new players in the programme.

The selected proposals will provide adapted support for Digital Europe Programme communication (including info days), dissemination and exploitation activities, including, for instance, the preparation of material and organisation of events.

Special attention should be given to enhancing the competence of NCPs, including helping less experienced NCPs rapidly acquire the know-how built up in other countries. Where relevant, synergies should be sought with existing networks to organise matchmaking activities.

13. DIGITAL-2023-SKILLS-04-BOOSTINGDIGIT (DIGITAL-CSA)

Boosting Digital Skills of young pupils, in particular girls

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-CSA DIGITAL Coordination and Support Actions	

Expected Outcome:
Stronger cooperation between primary, secondary and VET schools and tertiary education and research to increase the number of pupils enrolling in digital studies aiming at gender convergence. This will lead to the development of: Summer schoolsSpecialised information and career daysDissemination and outreach activities, such as EU Code Week.

Objective:
Students in digital and ICT disciplines represent a minority, in 2021 they were 4.5% of total graduates. There is also a severe gender balance issue, with only 19% of ICT specialists and one in three science, technology, engineering and/or mathematics (STEM) graduates being women. During the Structured Dialogue for digital education and skills, Member States also report about competition for the few pupils that have suitable profiles and interest in studying STEM disciplines at university level.
In order to fill the significant shortage of sector specialists using advanced digital technologies and ICT specialists, it is necessary to increase the pool of pupils who would be ultimately interested to study STEM and ICT, with a special focus on girls and women who are vastly underrepresented in the digital field. Boosting the development of digital skills from an early age and in a continuous manner is essential for influencing the level of digital skills of the EU population and the number of male and female students that will consider studies and career in the ICT. Moreover, evidence shows that pupils who are involved in the learning of coding or computational thinking from an early age are more likely to continue studying ICT or digital-related fields and this has an impact for example on the number of girls choosing this study-path.
In the bilateral dialogues with Member States as part of the structured dialogue on digital education and skills, many called for innovative approaches to attract young people, and especially girls as of primary school (or even earlier), to digital careers and to encourage a mind-set shift in their perception. This action will therefore include dedicated activities to encourage girls and women to take part in digital studies.

Scope:
The aim of this action is to pilot actions to increase the number of students pursuing digital studies and careers, with a special focus on increasing participation of girls. It will support joint actions between leading technical higher education institutions, businesses and schools to promote digital studies, through hands-on activities and challenge-based projects. Another aim of this action is to scale-up the EU Code Week initiative, putting it on stronger and broader footing, thus further increasing its impact beyond the > 4 million people reached every year, among which almost half are young women and girls.

For example, the actions will finance summer schools for high-school students on digital areas, career days for people interested in digital, with a view to encourage more gender diversity and promote exchanges between higher education institutions and primary and secondary schools on digital topics. Digital Europe Programme consortia already awarded under the first WP could also be leveraged, with a view to give the possibilities to younger students to access the state-of-the-art laboratories, experience the campus facilities and follow seminars from the most renowned experts in Quantum computing, Cybersecurity, AI, cloud, among others. Special attention should be given to the role of girls and women in the digital field, with a focus on debunking stereotypes and tackling the self-efficacy and confidence gap.

This action is in line with Action 13 of the Digital Education Action Plan (2021-2027), which aims to enhance girls and women's digital competences through projects like Girls Go Circular and ESTEAM Fests.

14. DIGITAL-2023-SKILLS-04-SEMICONDUCTORS (DIGITAL-SIMPLE)

Reinforcing skills in semiconductors

Status	Opening date	Deadlines	Funding type	Keywords
Open	11 may. 2023	26 sept. 2023	DIGITAL-SIMPLE DIGITAL Simple Grants	

Expected Outcome:
Concerning the projects addressing the Academic network (point I in scope above)
Definition of the required curricula using the ECTS system with capacity for around 500 students/year across at least 5 Member States, for BSc and MSc levels.A scholarship programme for selected semiconductors students enrolled in the common curriculum at BSc and MSc levels.On-the-job experiences for undergraduate students in companies involved in the consortium.Upgrade of laboratories used for the teaching activities delivered by the project.Communication initiatives toward the public, including social media.Local or regional programmes led by the industrial partner(s) to target secondary school students, including for example a Summer/Winter School based on practical learning activities, introductory seminars, visit to facilities etc.
Concerning the projects addressing the Vocational training (point II in scope above)
Bootcamps, workshops and career days dedicated to semiconductors, addressing start-ups and SMEs needs, at least one of them focusing on diversity and inclusivity.Definition of VET curricula in semiconductors and delivery of the relevant training courses with capacity for around 1000 technicians involving at least 20 start-ups and SMEs across at least 5 Member States.

Objective:
The share of students choosing ICT and notably semiconductors disciplines is too low to satisfy the demand required by the labour market. It is estimated that the BRIICS countries (including Indonesia) will produce three-quarters of the global STEM graduates by 2030 while Europe will be lagging well behind with an 8% share[1]. The shortage of potential employees with specific knowledge in semiconductors, and in particular the negligible share of students willing to undertake this field, has many different causes related to the low awareness of the impact of semiconductors in the society and citizens' daily life, and to low expectations in terms of prospective career and employment conditions. The problem is acute, given the gap between the labour market demands and the unavailability of both technicians and high-level graduates, and it is even more exacerbated by a strong gender imbalance.

The image of semiconductors related jobs needs to be improved in this regard with a holistic approach by industry and academia, jointly addressing: The low awareness of the public, and particularly the younger generation, of the social importance of semiconductors and its benefits for the whole society, i.e., for the green and digital transition or the targets set by the Chips Act.The awareness gap on future work commitments and employment conditions. It is well known that studies are greatly influenced by students' previous experience within the secondary school and in their private lives, which can hardly provide insight into this high-tech sector. Starting from the very first classes in secondary schools is of the greatest importance for targeting students interested to approach these disciplines, with particular focus on female students.The obstacles faced by companies, in particular SMEs given their limited means, to get the required talents, by setting up initiatives to attract both technicians and graduates, and bridge the gap between education and their labour demands.The need to provide updated academic curricula both in theoretical knowledge and lab experience on cutting edge topics - the high pace of advancements in the semiconductor sector forces upgrades that are difficult to implement by private and public universities, and liaison with industrial stakeholders is essential to access new technologies, launch educational opportunities and increase their attractiveness to students.The need of continuing vocational training to enhance employability, supporting personal development and encouraging re- and up-skilling. Technicians must be provided with additional training during their lifelong careers to keep up to date with new technologies and techniques.

Scope:
Consortia can apply for one or both the actions described below.
Academic network
The proposed project is required to develop a European Semiconductors Skills Academy: a European network of higher education institutions and relevant industries, including start-ups and SMEs in microelectronics, to address the above issues.

The Academy must strive for collective actions to increase the visibility and the attractiveness of existing curricula already run by the members of the consortium. In particular, focus should be on increasing the number of enrolled students coming from secondary schools and ensuring the availability, in higher education institutions' curricula, of topics addressing industry's needs as well as cutting-edge topics in the sector, for example Chip Design.

The Academy should address, for example:
the identification of relevant courses, jointly vetted with the industry partners, starting from existing curricula, or from newly selected cutting-edge topics, which should eventually lead to an automatic recognition of the European Credit Transfer System (ECTS) across universities, facilitating students' and workers' mobility and competence recognition across Member States;the upgrade of university laboratories for the delivery of the courses identified;cooperation agreements resulting in hands-on experiences in industry and financed by industry as part of the student curricula;the involvement of start-ups and SMEs as beneficiaries of students' mobility;communication actions and initiatives aimed at the general public as well as specific activities for the promotion of studies in semiconductors in local areas, particularly aimed at secondary school students.

Vocational training
The proposed project is requested to define a platform among Vocational and Educational Training (VET) centres, industry, in particular start-ups and SMEs, academia, and social partners to address the need of continuing vocational training to enhance employability. Notably, the platform will support innovative approaches to attract talents and re-/up-skill workforce for start-ups and SMEs, for example, through:
the identification of relevant training contents, jointly vetted with the industry partners;bootcamps on specific semiconductors topics vetted by and including start-ups and SMEs;training curricula implying the involvement of SMEs as beneficiaries of technicians' mobility;recognition of specific hard and soft semiconductors VET curricula across Europe;addressing the gender dimension of employability in the sector;apprenticeships in start-ups and SMEs and online training addressing employability for migrants and immigrants.

[1]"Education Indicators in Focus N°31" by the OECD, 2015.

15. DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION (DIGITAL-JU-SIMPLE)

Support for implementation of EU legislation on cybersecurity and national cybersecurity strategies

Status	Opening date	Deadlines	Funding type	Keywords
Open	25 may. 2023	26 sept. 2023	DIGITAL-JU-SIMPLE DIGITAL JU Simple Grants	

Expected Outcome:

Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole. Better compliance with NIS2 (Directive (EU) 2022/2555) and higher levels of situational awareness and crisis response in Member States. Organization of events, workshops, stakeholder consultations and white papers.Enhanced cooperation, preparedness and cybersecurity resilience in the EU.Support actions in the area of certification.

Objective:
The action focuses on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislation on cybersecurity in particular the NIS2 Directive (Directive (EU) 2022/2555), the Cybersecurity Act and the proposed Cyber Resilience Act, and the Directive on attacks against information systems (Directive 2013/40). It complements the work of SOCs in the area of threat detection. It is a continuation of work currently supported under the previous WP.

In addition, the action also aims at improving industrial and market readiness for the cybersecurity requirements set in the proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act bolstering cybersecurity rules to ensure more secure hardware and software products.

Proposals should contribute to achieving at least one of these objectives;
Development of trust and confidence between Member States.Effective operational cooperation of organisations entrusted with EU or Member State's national level cybersecurity, in particular cooperation of CSIRTs (including in relation to the CSIRT Network) or cooperation of Operators of Essential Services including public authorities.Better security and notification processes and means for Operators of Essential Services and for digital service providers in the EU.Better reporting of cyber-attacks to law enforcement authorities in line with the Directive on attacks against information systems.Improved security of network and information systems in the EU.More alignment of Member States' implementations of NIS2 (Directive (EU) 2022/2555).Support cybersecurity certification in line with the Cybersecurity Act.

Scope:
The action will focus on the support of at least one of the following priorities:
Implementation, validation, piloting and deployment of technologies, tools and IT-based solutions, processes and methods for monitoring and handling cybersecurity incidents.Collaboration, communication, awareness-raising activities, knowledge exchange and training, including through the use of cybersecurity ranges, of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555).Twinning schemes involving originator and adopter organisations from at least two different Member States to facilitate the deployment and uptake of technologies, tools, processes and methods for effective cross-border collaboration preventing, detecting and countering Cybersecurity incidents.Robustness and resilience building measures in the cybersecurity area that strengthen suppliers' ability to work systematically with cybersecurity relevant information or supplying actionable data to CSIRTs.Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle.Ensure a coherent cybersecurity

framework, facilitating compliance for hardware and software producers.Enhance the transparency of security properties of products with digital elements.Enable businesses across all sectors and consumers to use products with digital elements securely.Support to Cybersecurity certification, including support to national cyber authorities and other relevant stakeholders, such as SMEs.
The support will target relevant Member State competent authorities, which play a central role in the implementation of NIS2 (Directive (EU) 2022/2555), as well as other actors with the scope of this Directive.

The action may support amongst other the continuation of the kind of cybersecurity activities funded through the CEF Telecom programme, building where relevant on the results from the CEF projects.

Support will be provided amongst other for the on boarding to the CEF Cybersecurity Core Service Platforms of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555) and are potential users of the CEF Cybersecurity Core Service Platforms.

The action also supports industry, with a particular focus on start-ups and SMEs, to seize the industrial and market uptake opportunities given by the proposed Cyber Resilient Act and Cybersecurity Act.

16. DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST (DIGITAL-JU-GFS)

Preparedness support and mutual assistance

Status	Opening date	Deadlines	Funding type	Keywords
Open	25 may. 2023	26 sept. 2023	DIGITAL-JU-GFS DIGITAL JU Grants for Financial Support	

Expected Outcome:
Preparedness support servicesthreat assessment and risk assessment servicesrisk monitoring servicesmutual assistance among Member States.

Objective:
This mechanism aims to complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, by assisting Member States in their efforts to improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise.

The mechanism should also support mutual assistance between Member States for both preparedness and incident response actions.

Scope:
The provision of preparedness support services (ex-ante) shall include activities listed below:
Support for testing of essential entities operating critical infrastructure for potential vulnerabilities. Development of penetration testing scenarios for MS cybersecurity infrastructure (including infrastructure of Operators of Essential Services, Digital Service Providers and Governmental entities). The proposed scenarios should cover Networks, Applications, Virtualization solutions, Cloud solutions, Industrial Control systems, and IoT.Support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities.Support the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises such as the development of standardised cyber-ranges or other testing facilities, able to mimic features of critical sectors (e.g., energy sector, transport sector etc.) to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant.Evaluation and/or testing of MS cybersecurity capabilities (including capabilities to prevent, detect and respond to incidents).Consulting services, providing recommendations on how to improve infrastructure security and capabilities. Support for threat assessment and risk assessment. Threat Assessment process implementation and life cycle.Customised risk scenarios analysis. Risk monitoring service. Specific continuous risk monitoring such as attack surface monitoring, risk monitoring of assets and vulnerabilities.
Preparedness actions should benefit entities in NIS2 (Directive (EU) 2022/2555) sectors (e.g., energy, transport, banking…) and entities in other relevant sectors, as well as including SMEs and start-ups. Also within scope are actions for mutual assistance among Member States, i.e., tailored and targeted short-term assistance upon request and depending on the specific needs arising from an incident.

17. DIGITAL-ECCC-2023-DEPLOY-CYBER-04-STANDARDISATION (DIGITAL-JU-CSA)

Standardisation in the area of Cybersecurity

Status	Opening date	Deadlines	Funding type	Keywords
Open	25 may. 2023	26 sept. 2023	DIGITAL-JU-CSA DIGITAL JU Coordination and Support Actions	

Expected Outcome:

Organization of events, workshops, stakeholder consultations, and production of white papers, all fostering the development of harmonised standards and conformity with requirements stemming from above mentioned legislative framework.Support for participation of relevant European experts in European and international cybersecurity standardization fora.

Objective:
The objective of this topic is to support further standardisation in the area of cybersecurity, notably in view of the implementation of the proposed Regulation on the Cyber Resilience Act (CRA), in particular with a view to improving the awareness and engage stakeholders in such standardisation work.

Scope:
The aim is to ensure wide stakeholder participation in standardisation activities in the area of cybersecurity, and in particular in relation to development of harmonized standards facilitating the implementation of the Cyber Resilience Act. This can be in the form of meetings, workshops and collaborative activities, involving the private as well as the public sector.

The Cyber Resilience Act (CRA) proposal aims to improve the internal market's functioning by mandating that all products with digital elements (hardware and software) will only be made available on the market if they meet specific essential cybersecurity requirements. In order to facilitate the implementation of the CRA, harmonised standards would be developed, which, if followed, would trigger the presumption of conformity with the CRA essential cybersecurity requirements to which they correspond. This will be complementary to actions by the National Coordination Centres, which will play a key role in reducing negative cross-border spillovers and subsequent costs to society to mitigate the risks associated with non-secure products.

18. DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE (DIGITAL-JU-CSA)

Coordination between the cybersecurity civilian and defence spheres

Status	Opening date	Deadlines	Funding type	Keywords
Open	25 may. 2023	26 sept. 2023	DIGITAL-JU-CSA DIGITAL JU Coordination and Support Actions	

Expected Outcome:
Concrete activities such as discussions, meetings, white papers, workshops, which strengthen the links between the cybersecurity civilian and defence spheres.Synergies between these communities, such as common activities to exchange know-how and information.

Objective:
The objective is to enhance exchange and coordination between the cybersecurity civilian (including CSIRTs, law enforcement and cyber diplomacy communities) and defence spheres. This should in particular foster synergies between cybersecurity actions in Horizon Europe, Digital Europe and defence related actions carried out by the Union through its bodies and programmes, such as the European Defence Agency and the European Defence Fund.

Scope:
The aim is to organise activities that foster exchange with regards to cybersecurity technologies that have relevance in both civilian and defence context: meetings, workshops and collaborative activities between stakeholders of the civil and defence communities, addressing all stakeholders (academic, SMEs, industry, public authorities, etc.).

19. DIGITAL-ECCC-2022-CYBER-B-03-SOC (DIGITAL-JU-SIMPLE)

Capacity building of Security Operation Centres

Status	Opening date	Deadlines	Funding type	Keywords
Open	25 may. 2023	6 jul. 2023	DIGITAL-JU-SIMPLE DIGITAL JU Simple Grants	

Expected Outcome:

Outcomes and deliverables

Several cross-border platform(s) for pooling data on cybersecurity threat between several Member States, equipped with a highly secure infrastructures and advanced data analytics tools;World-class SOCs across the Union, strengthened with state of the art technology in areas such as AI;Sharing of Threat Intelligence between SOCs, and information sharing agreements with competent authorities and CSIRTs;Threat intelligence and situational awareness capabilities supporting strengthened collaboration in the framework of the Blueprint/CyCLONe and the Joint Cybersecurity Unit, as well as with law enforcement and defence.

Objective:

The objective will be to create, support and/or strengthen and interconnect SOCs at regional, national and EU level. This will allow for reinforced capacities to monitor and detect cyber threats, the creation of collective knowledge and sharing of best practices. In addition, data and capacities related to cybersecurity threat intelligence will be brought together from multiple sources (such as CSIRTs and other relevant cybersecurity actors) through cross-border platforms across the EU. The use of state-of the-art AI, machine learning capabilities and common infrastructures will make it possible to more efficiently and more rapidly share and correlate the signals detected, and to create high-quality threat intelligence for national authorities and other stakeholders, thus enabling a fuller situational awareness and a more rapid reaction.

Scope:

The aim is to improve cybersecurity resilience with faster detection and response to cybersecurity incidents and threats at national and EU level through the establishment of SOCs, leveraging disruptive technologies, and sharing of information leading to increased situational awareness and stronger EU supply chains. Specifically:

Supporting existing SOCs or establishing national, regional or sectoral SOCs serving private (SMEs in particular) and/or public organisations with real-time monitoring and analysis of data from public internet network traffic to detect malicious activities and incidents that affect the resilience of network and information systems;Strengthening SOCs by leveraging state of the art Artificial Intelligence (including Machine Learning techniques) and computing power to improve the detection of malicious activities, and dynamically learning about the changing threat landscape;Supporting information sharing among public authorities (including competent authorities and CSIRTs under the NIS Directive), as well as with other SOCs (e.g. operated by private entities), facilitated through appropriate sharing agreements, while complying with all obligations related to privacy and personal data protection;Developing and deploying appropriate tools, platforms and infrastructures to securely share and analyse large data sets among SOCs. Where possible and appropriate, existing building blocks will be re-used, including the results of relevant Connecting Europe Facility and Horizon 2020 projects;Supporting the increased availability, quality, usability and interoperability of threat intelligence data among SOCs and relevant entities;Identify potential critical dependencies on foreign suppliers and solutions in the area of threat intelligence and develop an EU supply chain on threat intelligence;Provide Member States bodies with threat intelligence and situational awareness capabilities helping to anticipate and respond to cyber-attacks, notably in the framework of the Blueprint/CyCLONe and the Joint Cybersecurity Unit;Bridge cooperation between various cybersecurity communities, e.g. civilian cybersecurity resilience, law enforcement, defence, taking into account cooperation frameworks such as the Blueprint/CyCLONe and the Joint Cybersecurity Unit.

To achieve this aim, the following activities are foreseen:
Grants will be made available to enable capacity building, e.g. though the establishment or reinforcing of SOCs serving private or public organisations, leveraging state of the art technology such as artificial intelligence and dynamic learning of the threat landscapeA call for expression of interest will be launched to select entities in Member Statesthat provide the necessary facilities to host and operate cross-border platforms for pooling data on cybersecurity threat between several Member States (data potentially coming from various sources). The call for expression of interest will also build up the planning and design of necessary tools and infrastructures.Building on the call for expression of interest, a joint procurement will be launched to develop and operate capacities for the selected cross-border platforms, including advanced tools and infrastructures to securely share and analyse large data sets and threat intelligence among the selected cross-border platforms (e.g. highly-secure infrastructure or advanced data analytics aimed at significantly improving the ability to analyse large sets of data) .

20. DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE (DIGITAL-JU-SME)

EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges

Status	Opening date	Deadlines	Funding type	Keywords
Open	25 may. 2023	6 jul. 2023	DIGITAL-JU-SME DIGITAL JU SME Support Actions	

Expected Outcome:
The expected outcomes will be a strong capacity in the Member States to react in a coordinated way to large scale cybersecurity incidents, as well as top-level cybersecurity ranges offering advanced skills, knowledge and testing platforms

Objective:
The implementation of this topic has two main objectives:
To strengthen the capacity of cybersecurity actors in the Union to monitor cyber-attacks and threats and supply chain risks, to react jointly against large incidents, and to improve relevant knowledge, skills and training. This objective will be pursued through the implementation of the Blueprint and the future Joint Cyber Unit considering the important role of the Computer Security Incident Response Teams (CSIRTs) network and of the Cyber Crisis Liaison Organization Network (CyCLONe).To create, interconnect and strengthen Cybersecurity ranges at European, national and regional level as well as within and across critical infrastructures, including in but not limited to sectors covered by the NIS Directive , in view to share knowledge and cybersecurity threat intelligence between stakeholders in the Member States, better monitor cybersecurity threats, and respond jointly to cyber-attacks.

Scope:
Proposals addressing the first objective should build capacity of cybersecurity actors to react in a coordinated way to large scale cybersecurity incidents, while fostering the role of CSIRTs, the CyCLONe network, the future Joint Cybersecurity Unit, and taking into account the Blueprint.

Proposals addressing the second objective should support the creation, operation, capacity increase and/or uptake of cybersecurity ranges, as well as foster networking between them in view to develop cybersecurity skills and expertise in key technologies (e.g. 5G, Internet of Things, Cloud, Artificial Intelligence, industrial control systems) as well as application sectors (e.g. health, energy, finance, transport, telecommunication, agri-food production, resource management) including consideration to cascading effects across sectors. This action will aim to:
exchange knowledge between cybersecurity ranges and create common data repositories; support large-scale and cross-sector scenarios covering a wide range of adversaries and attack strategies, including for example cross centre serious gaming exercises; allow realistic traffic simulation that reflect network conditions; support structured training and cybersecurity exercises to prepare cybersecurity defenders at both public and private organisations to enhance the protection and resilience of critical infrastructures, enterprises and communications networks; enable the conduct of hybrid trainings engaging all levels relevant to detecting, mitigating and preventing cyber-attacks (tactical, operational, strategic) while creating an environment where they can train communication, coordination and decision making; provide additional services to stakeholders such as structured test methodologies, vulnerability database and forensic tools; develop of automated content delivery options supporting specific job profiles.

21. DIGITAL-ECCC-2022-CYBER-B-03-UPTAKE-CYBERSOLUTIONS (DIGITAL-JU-SME)

Uptake of Innovative Cybersecurity Solutions

Status	Opening date	Deadlines	Funding type	Keywords
Open	25 may. 2023	6 jul. 2023	DIGITAL-JU-SME DIGITAL JU SME Support Actions	

Expected Outcome:

The funding will:

Support the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.Provide and deploy up to date tools and services to organisations (in particular SMEs) to prepare, protect and respond to cybersecurity threats.Improve the security of open-source solutions (e.g. establishment of bug bounty programmes).

Objective:

To support the market uptake and dissemination of innovative cybersecurity solutions (notably from SMEs, as well as results from publicly-funded research in the EU), improve knowledge, and auditing of cybersecurity preparedness

Scope:

The focus will be on improving cybersecurity capabilities across the EU, notably for SMEs and public organisations, through both supply and demand support measures. This may include awareness raising measures (where relevant in line with activities promoted by ENISA), or marketplace platforms supporting interaction between suppliers and adopters of cybersecurity solutions and training.

The types of tools covered must include at least one of the following:

Cybersecurity protection services;Auditing of cybersecurity resilience of equipment and services;Security testing tools including static-analysis code scanning tools;Cybersecurity investigation tools, tracing the origins of cybersecurity threats;Incident response tools that fit into general operational and management cybersecurity strategies; Support to Coordinated Vulnerability Disclosure, in line with national policies where relevant;Funding and support for projects that improve and/or audit open source software, with regard to cybersecurity; Support for hackathons, cybersecurity challenges and conferences, and for engaging with relevant stakeholders including software development communities;Support to awareness raising, prevention, education, training, and gender balance in cybersecurity.

22. DIGITAL-2022-CLOUD-AI-B-03-AI-ON-DEMAND (DIGITAL-CSA)

Deployment of the AI-on-demand platform

Status	Opening date	Deadlines	Funding type	Keywords
Open	25 may. 2023	29 ago. 2023	DIGITAL-CSA DIGITAL Coordination and Support Actions	

Expected Outcome:
Outcomes and deliverables

Deliverables
The European AI-on-demand platform, including: A visible catalogue of AI resources that are made in Europe and trustworthyA one-stop shop to access AI tools for the European industry and for public administrationsA reference and trusted marketplace for trustworthy AI resourcesServices in support of the public procurement of AI solutionsInterconnections to computing resources, data spaces and Testing and experimentation facilities developed under this programmeEstablished links with the network of European Digital Innovation Hubs to provide access of AI tools to SMEs and the public administration throughout Europe. A governance mechanism in view of the future sustainability of the AI on demand platform.
Outcomes
Increased visibility to trustworthy innovations, in particular those made in Europe.Easy access to AI tools by public administrations and European industry (in particular SMEs).
Objective:
The objective of this action is to develop and deploy the AI-on-demand platform, providing the requirements and underlying mechanisms for such platform.

Scope:
The awarded project will develop and deploy the AI-on-demand platform, taking into account the proposed requirements and mechanisms to optimise the impact of the AI-on-demand platform.

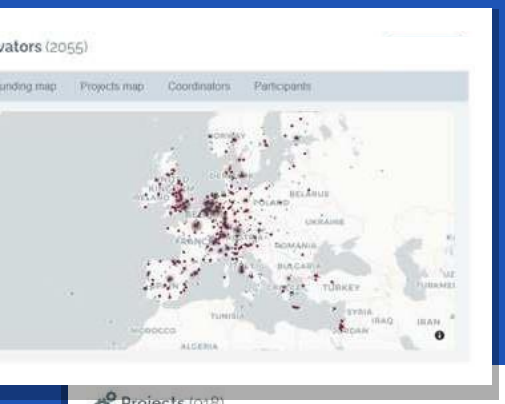
The platform will gather all the AI resources (algorithms and tools), and make them available to the potential users, businesses and public administration, with the necessary services to facilitate their integration. Activities shall build on results from the preparatory action, as well as previous relevant projects such as the AI-on-demand platform and the European Language Grid initiated under Horizon 2020. In addition, the platform should mobilise the European innovators to provide their products and services on the platform. The platform should become the reference for any user (industry or public service), a one-stop-shop to access AI tools to integrate into solutions, products, and services: a common good and market place for AI resources.

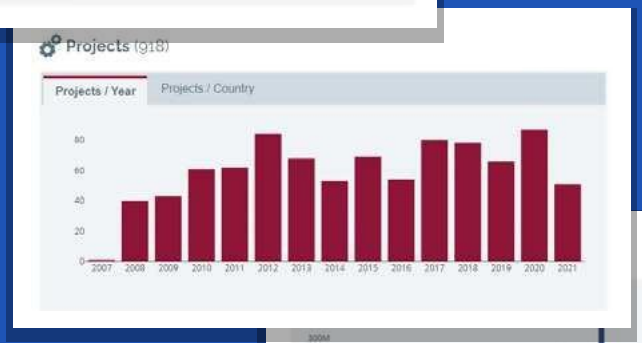
It will implement mechanisms defined in the preparatory action and further cooperate with the corresponding actions running in parallel to interconnect with the cloud-to-edge infrastructure, HPC resources, the data spaces, and the Testing and Experimentation Facilities (TEFs) – providing the TEFs with relevant AI and related resources, and hosting the results once validated in the TEFs, as applicable.

The platform will play the role of a central marketplace for AI tools, and a service layer providing support to users (incl. public administrations) for integration of AI solutions. In addition, it will bring the latest AI tools and solutions to the level of industrial standard requirements (code validation, quality check), connect to computing resources (e.g. HPC, cloud from this programme), data resources (e.g. data spaces from this programme, also datasets for training and validation), promote trustworthy AI development and deployment, facilitate the implementation of public procurement in AI, as well as raise awareness about best practices and success stories of AI applications in various domains. The AI-on-demand platform will also develop use-cases factory/library to support its activity. Specific attention will be given on guaranteeing that the resources on the platform respect the ethics guidelines issued by the High Level Expert Group on AI and the European AI Alliance and support the regulatory framework.

This document has been generated with Kaila,
a platform developed by ZABALA to foster open innovation.

Kaila is a collaborative hub that represents a paradigm shift in the management of innovation ecosystems, using advanced recommendation algorithms and the integration of main EU open data sources.





What can I do with Kaila?

- **Obtain funding for your projects**
- **Analyse innovation trends**
- **Competitive watch**
- **Find partners and collaborators**

Join for free