Grant Agreement N°: 956671

Topic: ICT-56-2020

The European IoT Hub

Growing a sustainable and comprehensive ecosystem for Next Generation Internet of Things

D2.6: NGIoT Roadmap and Policy Recommendations v2

Revision: 1.0

Work package	WP 2
Task	Task 2.3
Due date	31/03/2023
Submission date	19/04/2023
Deliverable lead	BluSpecs
Authors	Tanya Suárez (BluSpecs), Brendan Rowan (BluSpecs), Martín Robles (BluSpecs)
Version	2.0
Dissemination level	PUBLIC

Abstract

This report provides an analysis of two of the key drivers of the evolution of the NGIoT; research and innovation priorities from the tech developer communities and large legislative packages that will define the digital market over the coming decades. It provides a meta-analysis of key Strategic and Research Innovation Agendas representing 12 key industry and research associations, making a link to the Horizon Europe and Digital Europe Programmes. It covers an in-depth analysis of the impact on the NGIoT community of the upcoming Data, AI and Cyber Resilience Acts with recommendations for future Large Scale Pilots within the Cloud-Edge-IoT.

Keywords: Strategy, Innovation, Policy, Market, Skills, Pilots, Community

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	12/12/2022	Table of Contents	Brendan Rowan, BLU
V0.2	25/01/2023	First review of key policies – Update to Section 4	Martín Robles, BLU
V0.3	14/02/2023	First review of updated SRIAs – Update to Section 3.1	Martín Robles, BLU
V0.4	08/03/2023	Internal review	Brendan Rowan, BLU
V0.5	16/03/2023	Update to Section 3 – Data tables	Martín Robles, BLU
V0.6	23/03/2023	Complete Section 4	Martín Robles, BLU
V0.7	24/03/2023	Revision of Section 1 & 2	Brendan Rowan, BLU
V0.8	30/03/2023	Revision of Section 4	Tanya Suárez, BLU
V0.9	06/03/2023	Updated Section 4 Draft Conclusions Section 5	Tanya Suárez, BLU
V0.10	12/03/2023	Updated Section 3 – restructure and inclusion of Sections 3.4, 3.5	Brendan Rowan, BLU
V0.11	13/03/2023	Final version Section 5, Section 6	Tanya Suárez, BLU
V0.12	18/04/2023	Final draft provided	Brendan Rowan, BLU
V0.13	19/04/2023	Review	Eleni Pechlivanidou, Martel
V0.14	19/04/2023	Update	Brendan Rowan BLU
V1.0	20/04/2023	Final quality check and submission	Eleni Pechlivandou, Martel

Project co-funded by the European Commission under H2020		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g. web	X
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to EU-IoT project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
OTHER: Software, technical diagram, etc

EXECUTIVE SUMMARY

The Next-Generation IoT

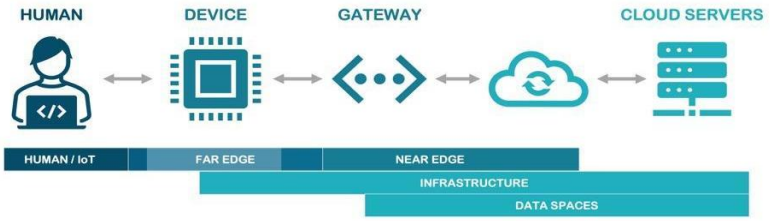
The NGIoT Initiative is focused on supporting the transition to the Cloud-Edge-IoT Continuum, driven by the orchestration of cloud and edge technologies which are in turn facilitated by the increased computing power available on chips and devices and the realisation of the collaborative IoT enabled by 5G technologies.

The Next-Generation IoT is characterised by a set of properties driven by the convergence of the edge and cloud and which may include:

- Federated architectures designed for distributed or swarm intelligence and federated services.
- Intelligent devices with hardware accelerators for on-device processing.
- Integration of microservices which support trust and security functions.
- Novel human-IoT interfaces such as AR and haptic responses.
- Leveraging of 5G management with network functional virtualisation and slicing.
- Management of public cloud and edge environments in the same application

A Framework for Assessing the NGIoT

To properly understand and analyse the needs of such a diverse and ever-growing community, the application of an EU-IoT framework captures the core requirements and needs, allowing for diversity, while taking into account the specific requirements of different cases It defines 5 contexts across the continuum on which the EU-IoT will focus: Human/IoT interface, Far Edge (devices level), Near Edge (gateway level), Infrastructure (including networks) and Data Spaces (cloud based and superlevel data sharing).



Reaching across the R&I Communities

Strategic Research and Innovation Agendas (SRIAs) are structured instruments that are built on the foresight and knowledge of experts actively developing the next generation of technologies, providing the common views and opinions of thousands of the leading European technology developers.

Within the scope of the identified target communities for the EU-IoT project and NGIoT Initiative[1], the latest publications, roadmaps and SRIAs were revised and reviewed. The main SRIAs which were analysed for key trends and themes across the contributing communities and NGIoT framework.

In total 645 topics were abstracted, categorised and analysed across two cycles and 590 assessed for defining the future demands for the NGIoT.

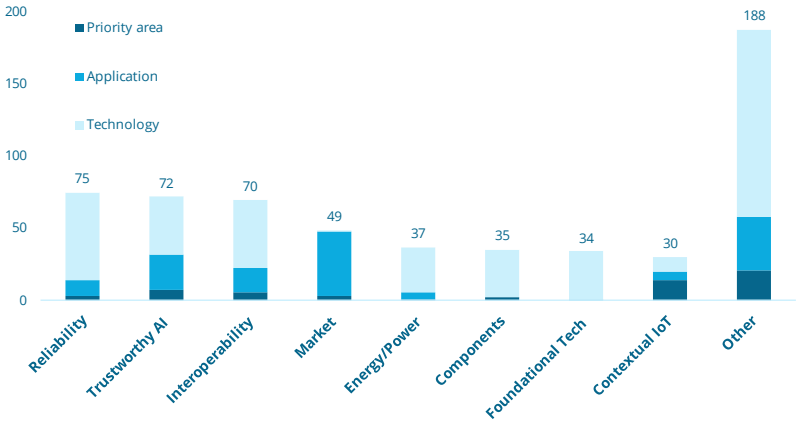
Key trends for the future of NGIoT and Edge

The advancement of the NGIoT Initiative has been a significant contributor towards the federation of devices, systems, and intelligence. The demand for interoperability at all levels and the deployment across heterogenous devices and systems heralds the arrival of the Cloud-Edge-IoT continuum and demand for distributed computing across networks and cloud environments.

Federation, addressing heterogeneity in devices, data, networks and cloud environments, distributed systems, and the interoperability of such systems defines the emergence of the continuum. The Cloud-Edge-IoT paradigm, significantly increases the complexity and dynamic nature of the computing systems. AI and ML, are seen as the tools for delivering performance and trust across the continuum, providing Self-X – self-organising, self-configuring, self-optimising, self-healing, self-adapting, self-management, self-updating – in evermore complex and context-aware environments.

The application of robustness and self-organization in response to incidents and ensure the continuity of service is a fundamental of the federated future. Without confidence of resource availability and assured redundancy, edge computing and distributed systems will remain solely in a research environment. Resilience and reliability of systems and associated security needs further development to deliver an industry ready, continuous deployment environment.

Beyond AI and federated and heterogenous systems there are emerging trends related to Green ICT, Sustainability of systems and devices, and a demand for tools and platforms to achieve the adoptability and application of the technologies.



The top 8 themes identified account for 68% of all topics, the majority of which refer to technologies to be developed. These eight leading themes are:

[1] D2.2 Towards a Vibrant EU IoT Ecosystem V2.0, 2022

- **Reliability:** encompasses the robustness of systems and the continuity of delivery, resource availability and performance.
- **Trustworthy AI**: addresses the development and adoption of trusted AI and ML based solutions. It covers both the leveraging of AI to support the functioning and security of systems and the increased confidence and adoption of existing and future distributed AI solutions.
- **Interoperability:** providing architectures, platforms, tools and networks that can handle heterogeneity and provide functionality across software and hardware.
- **Market Applications**: topics related to definition of use cases, specific societal challenges to be addressed and benefits to be realised, domain-based outcomes and the development of cross-vertical applications.
- **Energy/Power**: reducing the cost and consumption per bit processed and providing energy harvesting.
- **Components**: development of the building blocks for supporting the topics already identified above.
- **Foundational Tech**: topics in early TRLs of development and tend to have a long-term focus, e.g., quantum, silicon and radio frequency technologies and novel materials.
- **Other Topics**: includes Interfaces (XR and multimodal), Green ICT, Sustainability, Data Sharing, Approaches, Skills and Adoptability.

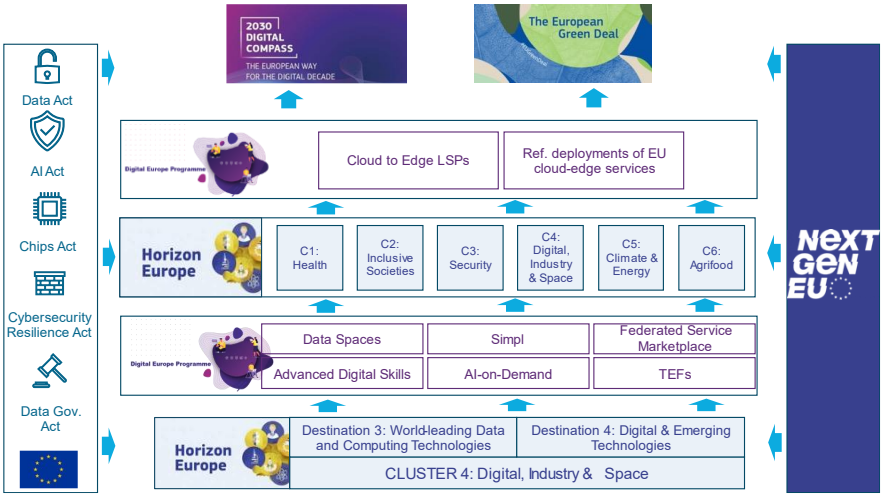
Preparing the market – beyond use cases

The emergence of a Cloud-Edge-IoT continuum, also presents new opportunities for new business models, however, the challenge remains to both clearly define and prove the business case behind the solutions under development with billions of euros of investment.

Continued work needs to advance on the market demand and the preparation of the industry adopters who need to make the case for investing in edge computing and the active participation in the ecosystems being generated through off-the-shelf models, digital twins, and Data Spaces. Skills and talent are wholly underrepresented across the board and must be addressed in the context of commercial feasibility.

Linking to Horizon and Digital Europe

Within this decade, the European Union, across Horizon Europe (€15.3 billion), DIGITAL (€7.5 billion), Next Generation EU (€38 billion), multi-county projects and IPCEIs, is putting its weight in the scale of billions of euros of investment behind the creation of a digital infrastructure.

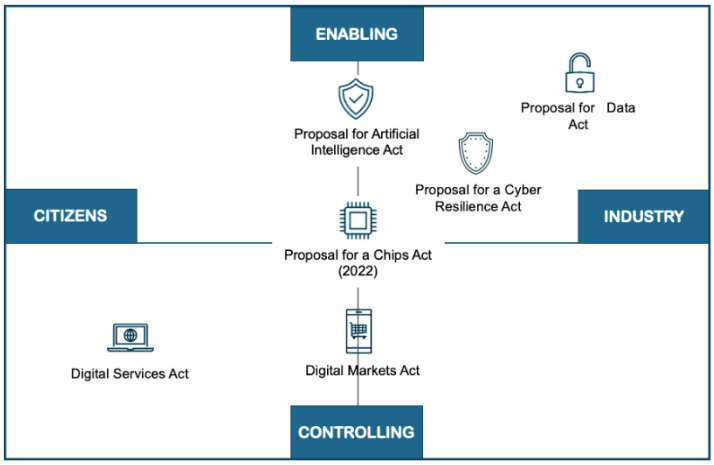


The positioning of the Cloud-Edge-IoT, and the development of the federated and autonomous system is evident as a foundational pillar for the realisation of key European aspirations to lead in digital. There is

an intercalation between the DIGITAL programme and the Horizon Europe activities which culminates in the Cloud-to-Edge Large Scale Pilots and the Reference Deployments

Policy analysis for Europe's Digital Decade

Across Europe, policymakers are launching initiatives to update existing regulatory and normative frameworks, adapting them to the all-pervasive digital economy that is shaping society, business, and even politics. Many of them will have a direct impact on the future of the next-generation IoT and the move to the Cloud-Edge-IoT paradigm.



The full impact of this significant level of investment into the digital economy will be contingent on the effective functioning of the Single Digital Market. In turn, this relies on the implementation of a harmonised regulatory[2] framework that can protect rights and provide guidance and legal certainty to all stakeholders. From this perspective, the most relevant regulations set to shape the NGIoT include:

- Proposal for Data Act {SEC(2022) 81 final}
- Proposal for Cybersecurity Resilience Act {SEC(2022) 321 final}
- Proposal for Artificial Intelligence Act {SEC(2021) 206 final}
- Digital Markets Act {Regulation (EU) 2022/1925}
- Digital Services Act {Regulation (EU) 2022/2065}
- Proposal for Chips Act {SEC(2022) 46 final}
- Proposal for Data Governance Act {SEC(2022) 868 final}

The Data Act is one of the regulations that is most likely to impact the Cloud-Edge-IoT Continuum, requiring several adjustments to the status quo; (i) requires adjustments to the purchase, leasing or renting agreements to clearly define how data is generated, used and made accessible, (ii) protect SMEs by ensuring fair terms of agreement within data sharing contracts.

For cloud and edge platform providers, it creates a significant set of obligations to enable the switching and multi-vendor environment for users through the portability of the assets.

The Cyber Resilience Act promotes security throughout IoT ecosystem and is an **essential step towards the increase AI Trustworthiness**. It encourages the **creation of a software bill of materials (SBOM),** which will help to provide transparency in exercising rights in the

AI Act: The categorisation of "AI systems" is central to the Act, imposing varying degrees of regulation according **to three risk categories**: **Unacceptable risk, High-risk applications, Non-high-risk**. It will result in the development of conformity assessment and harmonized standards, regulatory sandboxes and market supervision and coordination.

The Digital Services package will have an impact on NGIoT, particularly to companies that may

[2] A "regulation" is a directly applicable form of EU law, which has binding legal force in all member states. National governments do not have to take action to implement EU regulations. A "directive" is a legislative act setting a goal to be achieved by all EU countries, but leaving the method to each member state.

become designated as "gatekeepers" under the Digital Markets Act and the innovation and competition potential from the **limit on them.** The Digital Services Act may have a positive impact on the IoT research and innovation environment by promoting trust and confidence in online platforms through online safety and security.

Calls to action

The policy landscape is far from static, with several regulations still requiring the final seals of approval by the Union's legislative bodies. Once approved, certain regulations, such as the AI Act, will still be subject to regular reviews to allow for the rapid evolution of technology.

As things stand, the large-scale pilots present across Horizon Europe and Digital Europe can take some pre-emptive measures to support future compliance:

- Opportunities to develop new products & services independently of core platform providers.
- Capacity to demonstrate added-value services through start-up and SME engagement.
- Built-in compliance: solutions and standards to support functional data portability.
- Compliant high-risk AI systems.
- Study for monitoring and measurement of Data Act.
- Full vertical integration and large-scale investments.
- Investing in market readiness.
- Templates & tools for advanced CE marking and certification.
- Collaborative and active regulator engagement.

TABLE OF CONTENTS

1 INTRODUCTION 15
1.1 PURPOSE 15
1.2 CONTEXT 15
1.3 PRIOR READING 15
2 THE NEXT GENERATION IOT 17
2.1 OVERVIEW 17
2.2 TECH, MARKET, SKILLS AND STANDARDS IN THE HUMAN TO CLOUD CONTINUUM 18
3 STRATEGIC TOPICS AND THEMES RELATED TO THE NGIOT 20
3.1 RELEVANT STRATEGIC RESEARCH AND INNOVATION AGENDAS 20
3.2 METHOD AND APPROACH 21
3.3 PRINCIPAL OBSERVATIONS 22
3.3.1 General trends 22
3.3.2 Priority themes 23
3.4 CONTEXTUALISATION WITHIN THE NGIOT FRAMEWORK 27
3.5 LINKS TO HORIZON EUROPE AND DIGITAL WORK PROGRAMMES 29
4 POLICY ANALYSIS 32
4.1 A NEW AGE FOR DIGITAL POLICY DEVELOPMENT 32
4.2 NON REGULATORY MEASURES DRIVING NGIOT ADOPTION 32
4.3 REGULATORY MEASURES SHAPING THE NGIOT 34
4.4 THE DATA ACT 35
4.4.1 Purpose and scope 35
4.4.2 Main exclusions and limitations 35
4.4.3 Implications for the NGIoT 36
4.5 PROPOSAL FOR A CYBER RESILIENCE ACT (CRA) 39
4.5.1 Purpose and scope 39
4.5.2 Implications for the NGIoT 40
4.6 PROPOSAL FOR AN ARTIFICIAL INTELLIGENCE ACT 41
4.6.1 Purpose and scope 41
4.6.2 Implications for the NGIoT 42
4.7 THE DIGITAL SERVICES ACT PACKAGE 43
4.7.1 Scope, Purpose, and current status 43
4.7.2 Implications for the NGIoT 44
5 SUMMARISING OF IMPACT ON THE NG-IOT 46
5.1 RIGHTS AND OBLIGATIONS 46
5.2 DEFINING KEY ROLES (RELEVANT TO NGIOT) 50
5.3 THE COST OF NON-COMPLIANCE 51

6 CONCLUSIONS 53
6.1 THE ONWARD PROGRESS OF THE NGIOT 53
6.1.1 The era of federation and heterogeneity 53
6.1.2 Developing trust and resilience 53
6.1.3 Stimulating the competition to the top 54
6.1.4 Convergence across the digital sphere 54
6.2 POLICY CONSIDERATIONS THAT IMPACT THE ROADMAP 56
7 RECOMMENDATIONS AND CALLS TO ACTION 59
7.1 ACCESSING NEW RESOURCES AND CAPABILITIES 59
7.2 BUILT-IN COMPLIANCE 59
7.3 SUPPORTING A FUTURE-PROOF CEI 61
8 ANNEX 62

LIST OF FIGURES

Figure 1. Overview of the IoT NGIN meta-architecture (above) and high-level (below) demonstrating the integration of multiple technologies and microservices with novel and secure interfaces..... 18

Figure 2. The IoT continuum. From human to cloud and back again with key interfaces. 19

Figure 3. Guiding framework of the EU-IoT approach..... 19

Figure 4. Overview of the 6 Strategic Research and Innovation Agendas analysed and the contributing associations 21

Figure 5. Top themes present across SRIAs by number of categorised topics 24

Figure 6. Distribution of identified calls by level of relevance to NGIoT within each Cluster reviewed..... 30

Figure 7. Quantifying Spillovers of Next Generation EU Investment, Discussion Paper July 2021. European Commission. 33

Figure 8. Main regulations that are likely to have a direct impact on the NG-IoT..... 34

Figure 9. SBOM in the software cycle. Survey of Existing SBOM Formats and Standards (2021) NTIA. 40

Figure 10. Overview of the European panorama for Cloud-Edge-IoT 55

Figure 11. Mapping relevant regulation by focus and characteristics..... 56

Figure 12. Mapping relevant regulation onto the NG-IoT 57

LIST OF TABLES

Table 1. Summary of the dataset developed 22
Table 2. Distribution of contributors to each priority theme. Main contributor highlighted in blue. 24
Table 3. Distribution of all topics within the relevant SRIAs mapped against the EU IoT framework 27
Table 4. Distribution of topics within NGIoT contexts by source 28
Table 5. Distribution of themes within each NGIoT context. 28
Table 6. Summary of identified calls in the current Horizon Europe Work Programme 29
Table 7. Distribution of potential pilots and demonstrators for the Cloud-Edge-IoT Continuum. 30
Table 8 Comparison in scope (Article 1) between Initial proposal and the March 13th Parliamentary Approved Proposal 62

ABBREVIATIONS

AI	Artificial Intelligence
AB	Advisory Board
AR	Artificial Reality
BEREC	Body of European Regulators for Electronic Communications
BIM	Building Information Modelling
CB	Coordination Board
CTF	Communication Task Force
DID	Decentralised Identifier
CB	Coordination Board
CEI	Cloud-Edge-IoT Continuum
CSA	Coordination and Support Action
CTF	Communication Task Force
DEI	Digitising European Industry
DEP	Digital Europe Programme
DLTs	Distributed Ledger Technologies
EC	European Commission
ECUs	Electronic Control Units
EDPIA	European Digital Payments Industry Alliance
EG	Expert Groups
HPC	High-performance computing
HEP	Horizon Europe
IA	Innovation Actions
IAAS	Infrastructure-as-a-service
IETF	Internet Engineering Task Force
IoT	Internet of Things
IRTF	Internet Research Task Force
JU	Joint Undertaking
LEO	Low-Earth Orbit
MANO	Management and Orchestration
M2M	Machine to Machine
MR	Mixed Reality
NFV	Network Functions Virtualisation
NGI	Next Generation Internet
NGIoT	Next Generation Internet of Things
OECD	Organisation for Economic Co-operation and Development
OTA	Edge, over-the-air
RIA	Research and Innovation Actions
R&I	Research and Innovation
SDO	Standards Development Organization
SME	Small and Medium Enterprise
SNS	Smart Networks and Services
SoS	System of Systems
SRIA	Strategic Research and Innovation Agenda
TTN	The Things Network
UAVs	Unmanned Aerial Vehicles
VR	Virtual Reality

Disclaimer

The information contained in this document is provided for informational purposes only and should not be construed as legal advice on any subject matter.

This information is:

- of a general nature only and is not intended to address the specific circumstances of any particular individual or entity
- not necessarily comprehensive, complete, accurate or up to date
- sometimes linked to external sites over which the authors have no control and for which no responsibility is assumed
- not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional).

1 INTRODUCTION

1.1 PURPOSE

This paper provides a brief overview of how the European IoT technology stack is evolving, and how the policy framework, currently under development, is likely to impact this evolution in the future. The aim is to provide recommendations that can help to develop processes and mechanisms that align policy objectives and competitive and ethical technological development.

It does not purport to be exhaustive, or to be a legal treatise on the rights and obligations but rather an ongoing, iterative analysis of the common strategic objectives contained in leading European cloud-edge technology roadmaps, and the potential impact of selected European regulations. It provides the regulatory and research and innovation context as the Next-Generation IoT transforms into to the Cloud-Edge-IoT Continuum.

1.2 CONTEXT

EU-IoT is a Coordination and Support Action (CSA) for a portfolio of projects funded under the Horizon 2020 ICT-56 'Next Generation Internet of Things' Research and Innovation Actions (RIAs). These RIAs are tasked with developing and trialling next-generation architectures that underpin the deployment and accelerated development of edge computing, distributed intelligence, federated microservices, collaborative IoT and tactile interfaces integrating holistically enabling technologies such as DLTs and 5G.

These projects were awarded towards the end of the last Research and Innovation Framework Programme, Horizon 2020, as the IoT was evolving from a relatively delineated field and scope towards a computing continuum, from human to cloud. While the previous decade can be categorised by the widescale adoption of cloud computing and the rise of the hyperscalers, that have enabled much of the digital transformation, the next decade is expected to see the rise of edge computing, enabling a more distributed approach to data and intelligence.

The NGIoT Initiative is focused on supporting the transition to the Cloud-Edge-IoT Continuum, driven by the orchestration of cloud and edge technologies which are in turn facilitated by the increased computing power available on chips and devices and the realisation of the collaborative IoT enabled by 5G technologies.

It will lead to the processing of data closer to the source, with hyper local models being deployed in parallel to cloud-based models of models approaches. The human interface is expected to be less screen-based, as humans interact with devices in a myriad of ways, even becoming part of the AI decision-making process. This in turn is expected to increase trust and confidence in the next generation internet.

With the advances and increasing pervasiveness of digital technologies and ever-increasing rates of deployment, Europe is amid a legislative renewal with many aspects of digital technologies, services and markets being re-evaluated. The aim is to update existing regulations, adapting them to how technologies are known to impact society and business, but also to develop a future-proof approach that can be updated as technology continues to evolve. This will have a direct impact on shaping the future of the next-generation IoT in the Cloud-Edge-IoT Context.

Alongside this, is the launch of a set of new policy instruments: Horizon Europe, Digital Europe and the Recovery and Resilience Fund providing access to a significant pool of resources to shape Europe's digital future.

1.3 PRIOR READING

This document provides an overview of the main policies and trends affecting the transition to the

Cloud-Edge-IoT (CEI) paradigm. Several strategic roadmaps which offer projections and priorities for research and innovation have recently been published by leading European stakeholders. Their content will not be duplicated here but matched to the dynamic policy measures that are currently under development.

NGIOT: Roadmap for IoT Research, Innovation and Deployment in Europe 2021-2027[3]

This White Paper covers a definition and key domains within IoT and Edge Computing. It contains a sector overview with an analysis of the opportunities, barriers, and communities within each domain (Agrifood, Smart Cities, Health, Energy, Manufacturing, Automotive). The NGIoT Roadmap provides a tech-based approach to define key priorities and develops a series of recommendations that can be used as inputs to the Horizon Europe, Digital Europe and CEF 2 framework programmes.

EU-IoT produced mapping and analysis

- D2.5 NGIoT Roadmap and Policy Recommendations v1

This first version of the document identifies main research priorities and challenges providing an analysis and overview of the key impacts of the legislative pipeline. This current documents builds and advances on this.

- D2.2 Towards a Vibrant EU IoT Ecosystem V2.0

Provides an overview of the NGIoT technology landscape, identifies key challenges within the principal framework areas and provides the definition of the NGIoT Community and actors.

- D2.4 Expert consultation and dialogue report V2.0

Reports on engagement with experts on addressing the key challenges within the Data Act implementation and development of skills forecasts and profiles.

- D2.3 Expert consultation and dialogue report V1.0

Reports on engagement with experts on the validation of the EU IoT framework approach with inputs on technology maturity, and market drivers.

- D3.8 Recommendations on research priorities and innovation strategies to standardization v2.0

Presents the mapping of the key areas of standardisation and relevant bodies for the research and innovation activities across the ICT56 RIAs (NGIoT Initiative) building on the 18 months between previous version D3.7 and the ending of the project.

[3] IoT Research, Innovation and Deployment Priorities in the EU, White Paper, Version 2.0, (2022), Molina Castro F. *et al,* NGIOT CSA Consortium

2 THE NEXT GENERATION IOT

2.1 Overview

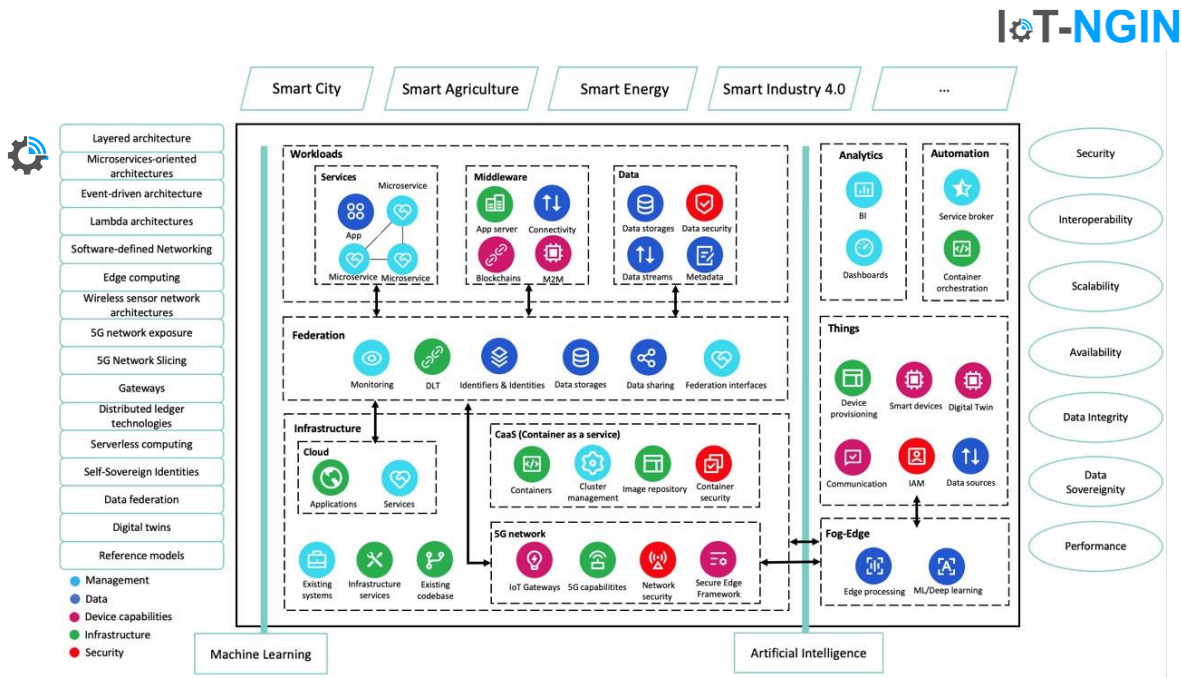
The exact definition of the IoT has been attempted by various bodies, from the IEEE definition based on a description of the constituent elements, to the ITU's definition focusing on what is achieves. The definition used in the NGIoT Roadmap encompasses both, describing the IoT as "*a system of systems that have (at least) the following properties: Sensing and actuation, Connectivity, Intelligence, Heterogeneity, Dynamicity, Scalability, Security*".[3]

At its most basic level, the IoT consists of a sensor which generates data, transmitted over a network to a central point for processing and abstraction of knowledge. But what differentiates the IoT from the NGIoT?

The Next-Generation IoT is characterised by a set of properties driven by the convergence of the edge and cloud and which may include:

- Federated architectures designed for distributed or swarm intelligence and federated services.
- Intelligent devices with hardware accelerators for on-device processing.
- Integration of microservices which support trust and security functions.
- Novel human-IoT interfaces such as AR and haptic responses.
- Leveraging of 5G management with network functional virtualisation and slicing.
- Management of public cloud and edge environments in the same application.

This is typified by the example meta- and high-level architecture of the IoT-NGIN RIA in the figure below.[4]



[4] D1.2 IoT meta-architecture, components, and benchmarking. September 2021. IoT NGIN Consortium

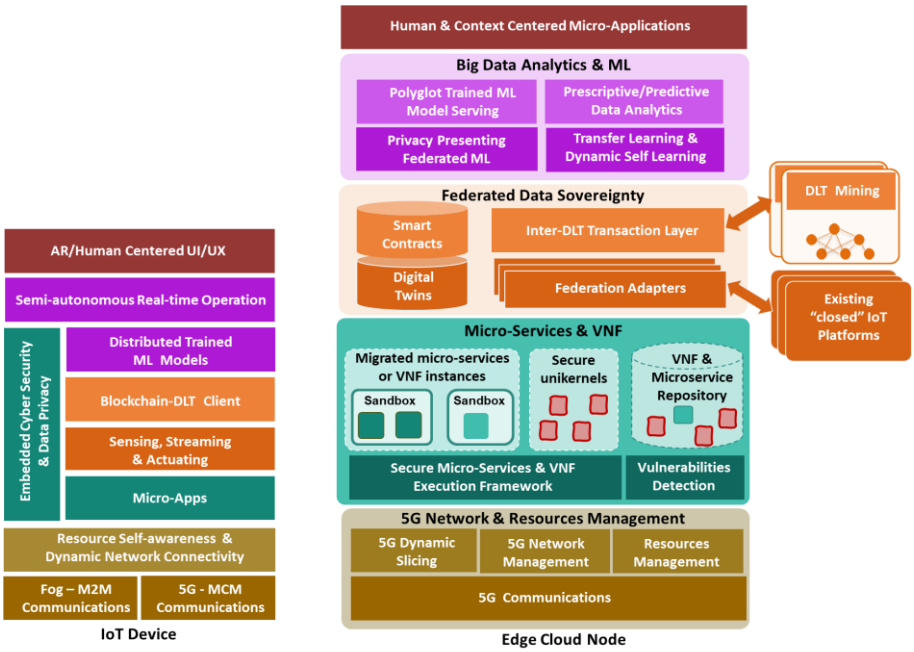


Figure 1. Overview of the IoT NGIN meta-architecture (above) and high-level (below) demonstrating the integration of multiple technologies and microservices with novel and secure interfaces

2.2 Tech, Market, Skills and Standards in the Human to Cloud Continuum

The European IoT landscape embraces several initiatives focusing on an increasing number of novel technologies across several verticals that allow for the proliferation of new IoT solutions and service models.

To properly understand and analyse the needs of such a diverse and ever-growing community, it is necessary to create a mapping process and a framework that allows EU-IoT to properly capture the core requirements and needs, allowing for diversity, while taking into account the specific requirements of different cases. Staying agile and being able to capture needs in a fast-changing context is a major factor influencing the design of the EU-IoT framework proposed below.

The first axis addresses the points of interaction between the physical elements which make up the human-to-cloud continuum, reflecting the current and future structure of the IoT. This axis considers the points of engagement and identifies areas and progression between and across them. These are defined within 5 contexts across the continuum on which the EU-IoT will focus: Human/IoT interface, Far Edge (devices level), Near Edge (gateway level), Infrastructure (including networks) and Data Spaces (cloud based and superlevel data sharing).

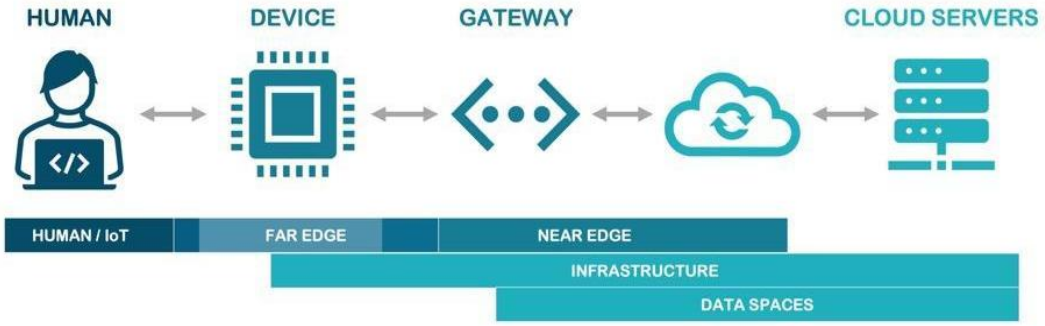


Figure 2. The IoT continuum. From human to cloud and back again with key interfaces.

Within these five key contexts, which frame advances, discussions, and debates, EU-IoT addresses four main layers of interest grouping important transversal aspects, as shown in Figure 3. Within each of these, there are several transversal themes and topics that will need to be addressed. These layers are:

- Technology: identifying novel and advancing enabling technologies.
- Market: analysing the applications, services, and models enabled by the technologies (both individual and varied combinations)[5].
- Standards and policies: delving into common approaches, standards, and policies.
- Skills: analysing the current and future demands resulting from all the above

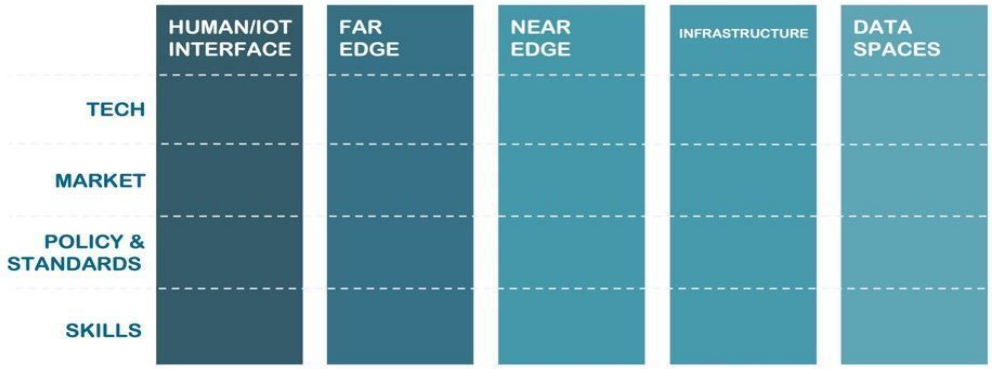


Figure 3. Guiding framework of the EU-IoT approach

[5] See NGIoT RIA's Call for Abstract Workshop on Market challenge: Reusability design for developed components.

3 STRATEGIC TOPICS AND THEMES RELATED TO THE NGIOT

3.1 Relevant Strategic Research and Innovation Agendas

Strategic Research and Innovation Agendas (SRIAs) are structured instruments that encapsulate the vision of an ecosystem of actors from research communities and industry bodies. They provide a scoping of the key priorities for collective investment and coordinated action within their technology fields for the coming years and are built on the foresight and knowledge of experts actively developing the next generation of technologies. As such, each SRIA represents the common views and opinions of hundreds of the leading European technology developers and provide a rich source for the identification of future challenges and priorities.

In order to provide the future progression from the NGIoT towards the already established Cloud-Edge-IoT Continuum[6], a meta-analysis of the relevant SRIAs here provides the guiding priorities and key trends for supporting the further deployment of the Horizon Europe and Digital Europe funding programmes.

Within the scope of the NGIoT initiative, the following SRIAs have been selected for analysis, cumulatively representing thousands of organisations and encompassing the spectrum from human to cloud:

- AIOTI Strategic Research and Innovation Agenda (Jan 23)
  - Alliance for Internet of Things and Edge Innovation
- Networld Europe Strategic Research and Innovation Agenda (Dec 22)
  - European Technology Platform (ETP) for communications networks and services, 6GIA, NESSI, AIOTI
- Electronic Components and System: Strategic Research and Innovation Agenda (Jan 22)
  - Aeneas, Artemis-IA, EPoSS
- European Industrial Technology Roadmap for the Next Generation Cloud-Edge Offering (May 21)[7]
  - European Alliance for Industrial Data, Edge and Cloud.
- Made In Europe: Horizon Europe Strategic Research and Innovation Agenda (Sep 2021)
  - European Factories of the Future Research Association
- Strategic Research, Innovation and Deployment Agenda, ADRA Partnership, September 2020:
  - BDVA/DAIRO, CLAIRE, ELLIS, EurAI, EURobotics

Other SRIAs that were reviewed and not included in this analysis are, Open Science in Europe, Build 4 people SRIA, and 2Zero emission transport. While they address some relevant elements, they are not considered to provide direct contributions to the NGIoT and Cloud-Edge-IoT. They may be, however, of interest with regards to identifying applications and use cases in smart buildings, logistics and transport. Similarly, The ETIP Smart Networks for Energy Transition

[6] The emergence of the EU Cloud Edge IoT Continuum and the role of the NGIoT is addressed in the following paper from UNLOCK CEI: Rowan, B, Álvarez, JE, & Kušíková, Z. (2023). Technology scoping paper (1.0). Zenodo. https://doi.org/10.5281/zenodo.7821363

[7] The Alliance is anticipated to produce in 2023 an updated roadmap, the latest from the Alliance can be found at https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance

(SNET), published their R&I Roadmap in March 2023 and explores highly relevant applications of the technologies within the NGIoT[8].

Figure 4. Overview of the 6 Strategic Research and Innovation Agendas analysed and the contributing associations

3.2 Method and approach

In performing the meta-analysis the following actions were taken to realise the comparison and data collection across the SRIAs and roadmaps:

- Within the scope of the identified target communities for the EU-IoT project and NGIoT Initiative[9], the latest publications, roadmaps and SRIAs were revised and reviewed. Selected SRIAs to be included met the following criteria:
  - Relevance to the scope of the NGIoT and latterly the Cloud Edge IoT Continuum.
  - Level of detail and structured representation.
  - Specificity and actionability of the topics provided.
- From the selected agendas, individual topics were abstracted and categorised under the following fields to provide a comparable analysis and assessment:
  - Type
    - Priority area: considered to be topics of strategic importance, encompassing multiple technologies and applications. E.g., Constraint-based planning and decision making in complex natural environments.
    - Application: specific implementations of technologies either within a given

[8] European Commission, Directorate-General for Energy, Strbac, G., Souza e Silva, N., Vasiljevska, J., et al., ETIP SNET, R&I Roadmap 2022-2031, Genova, E. (editor), Dimeas, A. (editor), Bacher, R. (editor), Karakitsios, J. (editor), Hatziargyriou, N. (editor), Trifiletti, M. (editor), Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2833/179516

[9] D2.2 Towards a Vibrant EU IoT Ecosystem V2.0, 2022

context or addressing a defined goal. E.g., Data streaming in constraint environments.

- Technology: a variety of different technical, electronic or physical systems, assets, devices or algorithms. E.g., Self-configuring and adaptive sensor nodes.

- Theme: definition of the common priority theme, taking a bottom-up approach and aligned with the NGIoT technologies.
- Position within the EU-IoT framework as described in the previous section:
  - Layer: Tech, Market, Policy & Standards, Skills, All.
  - Context: Human Interface, Far Edge, Near Edge, Infrastructure, Data Spaces, All.

- Finally, the analysis identified the key trends and themes across the contributing communities and NGIoT framework.

In total **645 topics were abstracted, categorised and analysed across two cycles**. The resulting database is provided as a public output for further analysis and reuse by the community and construction of future trend mapping. Within this paper, the latest versions of identified agendas were included in the analysis totalling 590 topics.

Table 1. Summary of the dataset developed

Source	Year	Nº Topics	Included
AIOTI Strategic Research and Innovation Agenda	2023	165	•
AIOTI Research and Partnership Perspective on Key IoT Areas	2021	10	
Networld Europe Strategic Research and Innovation Agenda	2022	175	•
Electronic Components and System: Strategic Research and Innovation Agenda	2022	159	•
Electronic Components and System: Strategic Research and Innovation Agenda	2021	45	
Made in Europe: The manufacturing partnership in Horizon Europe - Strategic Research and Innovation Agenda (SRIA)	2021	29	•
European industrial technology roadmap for the next generation cloud-edge offering	2021	20	•
Strategic Research, Innovation and Deployment Agenda: ADRA	2020	42	•
		645	**590**

3.3 Principal observations

3.3.1 General trends

Within the data, it is evident the maturation of AI from basic principles to applications and the emergence of both Edge processing and the Computing Continuum. Key concepts also observed

across all communities include Green ICT, Sustainability and Tools.

AI is required to underpin the development and management of autonomous and intelligent systems, be human-centred and interrogable and evermore efficient. There is an **omnipresence for AI topics** across all fields and a demonstrated need to provide the next-generation of **processors, interfaces, domain specific and cross-vertical agnostic models, niche and complex digital twins, the introduction of the concept of ´data for AI´, and the advancement of hybrid, swarm and distributed intelligence.**

Federation, addressing heterogeneity in devices, data, networks and cloud environments, distributed systems, and the interoperability of such systems is a particular highlight. It defines the emergence of the continuum, underpinned by cognitive, flexible, and contextual computing. AI and ML, are seen as the tools for delivering performance and trust across the continuum, providing **Self-X – self-organising, self-configuring, self-optimising, self-healing, self-adapting, self-management, self-updating – in evermore complex and context-aware environments.**

New topics are emerging under **Green ICT** which seeks to reduce the impact of the deployment of technologies, networks and data centres as well as putting technology to the service of society in **realising a lower footprint across industries**.

Similarly, the concept of sustainability of systems and devices is coming to the fore, addressing the **extension of the lifecycle through virtualisation and digital twins, integration and interoperability with legacy architectures and models**, and improving the recyclability of physical devices at end of life.

Finally, there is a demand for the tools and platforms to achieve the adoptability and application of the technologies. Developers require targeted **support to deploy solutions on the emerging dynamic, secure, robust, and integrated systems, to build in off-the-shelf and programmable modules and components across software and hardware**, supporting continuous delivery/continuous deployment.

3.3.2 Priority themes

Across the 590 topics analysed, 8 key themes were isolated as common priorities which account for a combined 68% of the total set. At the **top are the three themes of Reliability, Trustworthy AI, and Interoperability**. In comparison to previous analysis, Reliability has risen over 8 positions with the latest dataset and Trustworthy AI 3 positions. The presence of Market (applications, use cases and approaches) has increased overall and represents the strategic and applied nature of the tech development within the Cloud-Edge-IoT and NGIoT community.

Contextual IoT, while increasing in number of topics, has become smaller in relevance. It is perhaps, more a reflection of the refinement of the definition from responsive operations of devices to constrained or human-defined environments to a fuller concept of the dynamic and autonomous continuum that emphasises the reliability and quality of service, particularly in networks which cuts across other topic areas.

Noteworthy, is also the detail provided within topics, with more technologies being defined than previously identified. There is an overall ratio of 1:2.5:7 between Priority Areas: Applications: Technologies, compared to a previous ratio of 1:1:0.5 indicating a maturing of clarity and direction from the communities, for example, that provided within the Networld Europe and AIOTI contributions.

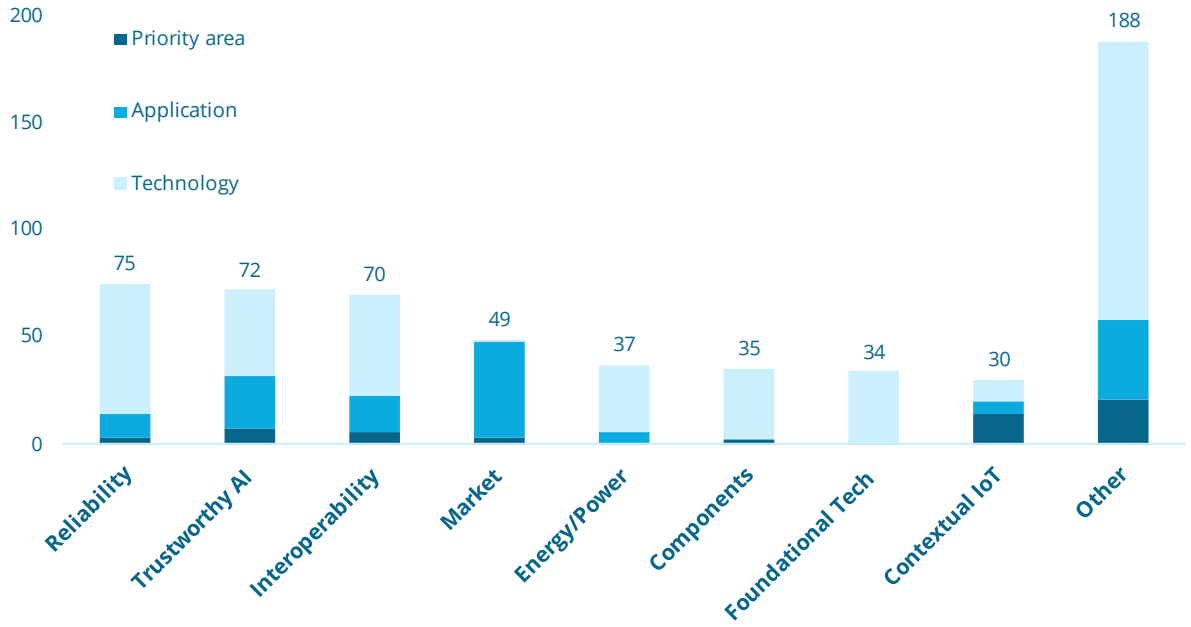


Figure 5. Top themes present across SRIAs by number of categorised topics

Table 2. Distribution of contributors to each priority theme. Main contributor highlighted in blue.

	Networld Europe	AIOTI	ECS	ADRA	EFFRA	Ind. Data, Edge & Cloud
Reliability	64%	19%	12%	3%	1%	0%
Trustworthy AI	21%	35%	24%	15%	6%	0%
Interoperability	9%	44%	37%	0%	9%	1%
Market	20%	6%	57%	0%	12%	4%
Energy/Power	45%	26%	18%	3%	0%	8%
Components	37%	20%	40%	0%	3%	0%
Foundational Tech	62%	0%	29%	0%	3%	6%
Contextual IoT	0%	30%	10%	50%	10%	0%
Other	24%	35%	24%	7%	4%	6%
Total	**30%**	**28%**	**27%**	7%	5%	3%

Reliability

Reliability and the technologies which provide this are a clear priority, especially within the network community. **Reliability encompasses the robustness of systems and the continuity of delivery, resource availability and performance**. Topics highlight the need to ensure the capacity for systems and solutions to **perform at scale without loss of quality, latency and speed and the prioritisation of critical process**. Included is the security and safety, and long-term viability of deployments. Compared to the next priority theme, it is primarily composed of technologies.

Examples include:

- Design for (EoL) reliability: virtual reliability assessment prior to the fabrication of physical HW.

- Virtualisation of security functions and application of frugal cryptography and XDR.
- Managing and orchestrating wireless/cellular networks parameters to provide priority for resources based on QoS, safety-, mission-critical features for IoT systems.
- Redundant, meshed, and flexible optical layer network architectures.
- Secure and intrinsically safe sensing systems.

Trustworthy AI

A diverse category, which addresses the development and adoption of trusted AI and ML based solutions. It covers both the **leveraging of AI to support the functioning and security of systems and the increased confidence and adoption of existing and future distributed AI solutions.** Topics look at improving the quality and management of data and knowledge in building models, the scaling and integration of existing models, the cross-vertical adaptations of trained models and the building of human interfaces as well as tackling decision-making processes. Within the theme of AI, there is a cross-cutting thread of **promoting and tackling challenges around federated learning, swarm computing and edge intelligence**.

Examples include:

- Understand effect of system heterogeneity on the AI model aggregation efficiency.
- Ensure applicability of traditional AI methods to swarm systems.
- AI/ML computing with and on transient/limited resources.
- Network Domain Automation via AI/ML assisted decision-making processes and issuing recommendations and improved resource allocation and function placement algorithms.
- Hybrid knowledge representation, techniques for hybrid decision making.
- Develop distributed and federated systems, using heterogeneous decision mechanisms targeted to specific QoS or vertical sectors.

Interoperability

The theme of interoperability looks not only at the level of devices, data and networks but across platforms, models (including digital twins), and whole systems. The demand is for providing architectures, platforms, tools and networks that can **handle heterogeneity and provide functionality across software and hardware.**

Interoperability also intersects with reliability of systems and the whole lifecycle management of systems with the application of modular architectures and virtualisation approaches.

Examples include:

- Develop algorithms for management of heterogeneity of hardware, software and AI
- Engineering process for interoperability along the lifecycle of SoS
- Co-design: algorithms, HW, SW and topologies
- Horizontal and vertical integration of IoT Digital Twins models.
- Create Edge IoT platforms that combine distributed architectures converging mesh, DLT and AI technologies.
- Develop multi-protocol, multi frequency modules for autonomous edge IoT devices and vehicles.

Market Applications

The theme of market applications is demonstrated by topics related to definition of use cases, specific societal challenges to be addressed and benefits to be realised, domain-based outcomes and the development of cross-vertical applications. It is composed principally by applications and more than half of the topics result from the ECS communities.

Examples include:

- Simulation and modelling (digital twins) covering the material processing level up to manufacturing system, and factory and value network level from design until recycling.
- Enhance access to personalised and participative treatments for chronic and lifestyle-related diseases.
- Zero-defect and first-time right production
- CI/CD automation use cases including organizational issues; Integration with business process.
- Vertical Specific Security Profiles: Completion of KPI set per vertical applications. This should encompass security levels and specific attack surface.
- Integrate swarms in multiple verticals sectors to demonstrate added value.

Energy/Power

Across chips, networks, cloud providers and IoT the increased efficiency of systems is a necessary focus. There is a **need to reduce the cost and consumption per bit processed** to reduce whole sector energy demand, support the operation of constrained devices, promote distributed intelligence and ensure the scalability and business cases for edge and cloud.

Topics address thermal management, resource optimisation, low power and energy harvesting.

Examples include:

- Create new low-power and very low latency protocols for in-swarm communication.
- Exploring offloading of computationally intensive and delay- sensitive workloads.
- Battery-free operation and disposable devices. Low or zero energy systems based on ambient energy.
- Petabit/s energy-efficient interconnections; Cost per bit and power per bit reduction.
- Architecture and processor trade-offs (TPU, GPU, CPU, DSP, ASIC, FPGAs, ASIPs,...).

Components

Within this theme is the development of the building blocks for supporting the topics already identified above. Topics centre on the hardware and software components that are required for advancing deployment of technologies and are key enablers.

Examples include:

- Programmable Integrated Photonic Processing hardware
- Ultra-massive MIMO
- Flexible and structural substrate electronics
- Embed advanced accelerator functionalities in edge devices
- Design hardware/software for next- generation intelligent, adaptive, and autonomous

edge IoT systems.

Foundational Tech

This covers topics, that unlike components, are in early TRLs of development and tend to have a long-term focus. It addresses quantum, silicon and radio frequency technologies and novel materials. For example, memory technologies towards the yottabyte area, 3D integration technologies, technologies for in-memory computing, high-performance, ultra-low power 3D integration.

Other Topics

Across the remaining topics the principal themes include Interfaces (XR and multimodal), Green ICT, Sustainability, Data Sharing, Approaches, Skills and Adoptability.

3.4 Contextualisation within the NGIOT framework

The distribution within the NGIoT framework, **demonstrates the significant emphasis on the development of technologies**, with over 75% of all topics located in this layer. Across the Market and Policy & Standards there is a similar volume of topics while **Skills remains lightly addressed**. When skills are addressed, it is either in broad terms such as skilled workforce or training, or looks at the role of low-code platforms for knowledge experts at the Human Interface.[10] EFFRA as the more industrial and application focused of the SRIAs analysed had the largest volume of Market topics; almost two thirds of all topics.

Table 3. Distribution of all topics within the relevant SRIAs mapped against the EU IoT framework

	HUMAN INTERFACE	FAR EDGE	NEAR EDGE	INFRA STRUCTURE	DATA SPACES	ALL	
TECH	14%	17%	11%	**26%**	4%	4%	**75%**
MARKET	**4%**	1%	1%	**4%**	2%	2%	13%
POLICY	2%	1%	2%	**3%**	2%	1%	11%
SKILLS	0.5%					0.5 %	1%

Across the contexts of the NGIoT, the largest number of topics is found within Infrastructure. While largely due the contribution of Networld Europe and the almost exclusive focus on that context by the represented 5/6G communities, there is however a significant contribution by both AIOTI and ECS, accounting for 14% and 21% of their total contributions respectively. This emphasises the **convergence and need for joint coordination in the management of next-generation networks that define the future of edge computing** and underpin the deployment of autonomous and federated systems.

A **clustering at the edge is observed between AIOTI and ECS**, suggesting a natural collaboration and coordination between the communities. This complementarity is further demonstrated in the distribution of themes within these two communities shown previously in Table 2 where they mutually complement one another across the top themes.

[10] EU-IoT has developed a skills and jobs roles framework to define the skills and jobs within the future IoT: J. Soldatos. (2023). The EU-IoT Framework for Internet of Things Skills: Closing the Talent Gap (V1.0). Zenodo. https://doi.org/10.5281/zenodo.7544732

Table 4. Distribution of topics within NGIoT contexts by source

	HUMAN INTERFACE	FAR EDGE	NEAR EDGE	INFRA STRUCTURE	DATA SPACES	ALL	
Networld Europe	8	8	6	**127**	2	24	175
AIOTI	29	**67**	31	23	15		165
ECS	**54**	20	39	33	10	3	159
ADRA	**23**	12	1	1	1	4	42
EFFRA	8	3	2	2	5	**9**	29
Data, Edge & Cloud		2	2	3	**10**	3	20

Across Human Interface, Far and Near Edge, the theme of Trustworthy AI is the largest. Both Interoperability and Contextual IoT follow in Human Interfaces and Far Edge, with Market Applications closely coming behind. The main differences observed occur in the right-hand set of contexts. Under Infrastructure, the largest concern is for Reliability and is also the context which calls for more investment in Foundational Tech. Within Data Spaces, the equal demand is across Interoperability, Approaches and Data Sharing. Finally, across the whole field, the emergence of Green ICT is evident.

Table 5. Distribution of themes within each NGIoT context.

	HUMAN INTERFACE	FAR EDGE	NEAR EDGE	INFRA STRUCTURE	DATA SPACES	ALL
Reliability	8%	8%	7%	**23%**	0%	**16%**
Trustworthy AI	**14%**	**18%**	**19%**	6%	2%	**16%**
Interoperability	**11%**	**13%**	**9%**	**15%**	**14%**	2%
Market	10%	9%	**10%**	5%	7%	**16%**
Energy/Power	2%	8%	5%	9%	9%	0%
Components	7%	7%	4%	6%	5%	7%
Foundational Tech	3%	0%	4%	**11%**	5%	12%
Contextual IoT	**11%**	**13%**	1%	1%	0%	0%
Interfaces	7%	8%	4%	1%	0%	0%
Sustainability	1%	0%	5%	5%	7%	9%
Green ICT	2%	2%	4%	2%	9%	**16%**
Approach	0%	1%	6%	3%	**14%**	0%
Data sharing	1%	3%	0%	3%	**14%**	0%
Other	21%	12%	23%	11%	14%	5%

3.5 Links to Horizon Europe and DIGITAL Work Programmes

In the Horizon Europe Work Programme 2023-2024, it is estimated that there is a total of €1.1billio assigned to topics relevant to the NGIoT and Cloud-Edge-IoT, anticipated to fund around 150 projects, 52% of which are Research and Innovation Actions, 44% Innovation Actions, and 4% Coordination and Support Actions.

There is a good coherence between the data within the SRIAs and the themes addressed within the Horizon Europe WP, with many of the topics addressed together within the scope of a single call. While although there appears to be many calls, only 40% show high relevance. A significant number relate to the demonstration of federated systems and distributed intelligence in general and do not address the development of components or underlying architectures.

Table 6. Summary of identified calls in the current Horizon Europe Work Programme

CLUSTER AND DESTINATION	BUDGET	CALLS	PROJECTS
1- Health	89.000.000,00 €	3	10
Unlocking the full potential of new tools, technologies and digital solutions for a healthy society	89.000.000,00 €	3	10
3 - Civil Security for Society	139.600.000,00 €	8	25
Increased Cybersecurity	119.100.000,00 €	5	21
Resilient Infrastructure	20.500.000,00 €	3	4
4 - Digital, Industry and Space	611.500.000,00 €	25	80
A human-centred and ethical development of digital and industrial technologies	245.000.000,00 €	12	33
Digital & Emerging Technologies for Competitiveness and Fit for the Green Deal	206.500.000,00 €	8	31
Increased autonomy in key strategic value chains for resilient industry	4.000.000,00 €	1	1
World leading data and computing technologies	156.000.000,00 €	4	15
5 - Climate, Energy and Mobility	215.700.000,00 €	17	31
Clean and competitive solutions for all transport modes	52.700.000,00 €	4	9
Cross-sectoral solutions for the climate transition	34.000.000,00 €	2	3
Efficient, sustainable and inclusive energy use	10.000.000,00 €	1	2
Safe, Resilient Transport and Smart Mobility services for passengers and goods	10.000.000,00 €	1	2
Sustainable, secure and competitive energy supply	109.000.000,00 €	9	15
6 - Food, Bioeconomy, Natural Resources, Agriculture and Environment	40.000.000,00 €	1	1
Innovative governance, environmental observations and digital solutions in support of the Green Deal	40.000.000,00 €	1	1
Innovative Europe	4.000.000,00 €	1	4
	1.099.800.000,00 €	**55**	**151**

Within the calls identified, those with highest relevance are found in Cluster 4, specifically within the three destinations of:

- A human-centred and ethical development of digital and industrial technologies

- Digital & Emerging Technologies for Competitiveness and Fit for the Green Deal
- World leading data and computing technologies

Across these Destinations examples of related calls include:

- Cognitive Computing Continuum
- Large Scale pilots on trustworthy AI data and robotics
- Piloting emerging Smart IoT Platforms and decentralized intelligence
- Efficient trustworthy AI - making the best of data
- Next Generation Internet Fund

Within these highly relevant calls, the **themes of Trustworthy AI and Interoperability are well addressed, especially with a market focus and the development of architectures, platforms, and tools**. It is noted, however, that there is a need for greater topics under Reliability given the number present across the SRIAs. It is similarly so for the theme of Energy/Power; while efficiency and scalability of AI is addressed in three calls, it is required to be addressed more strongly and overtly rather than as a cross-cutting priority.

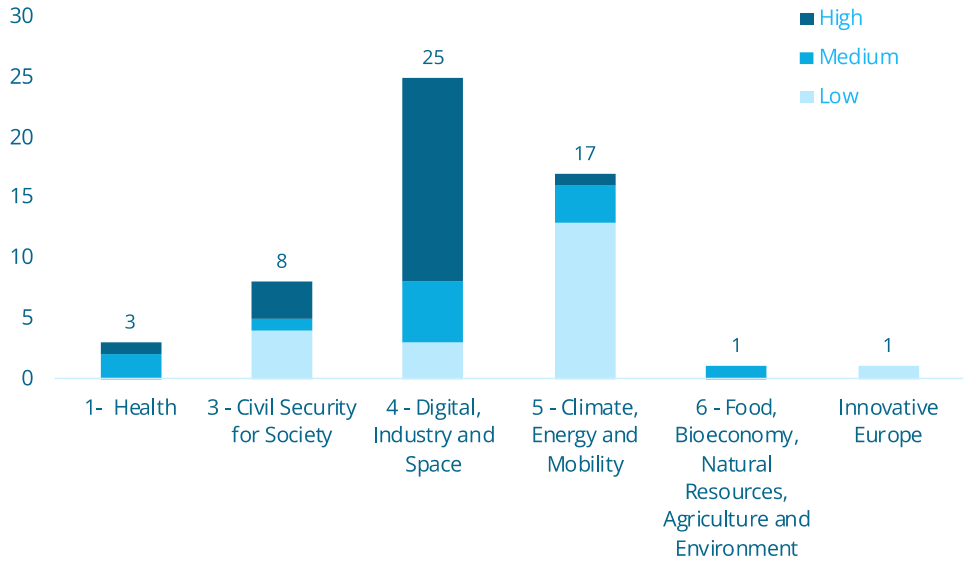


Figure 6. Distribution of identified calls by level of relevance to NGIoT within each Cluster reviewed.

As previously mentioned, the development and deployment of the Cloud-Edge-IoT Continuum is present across a number of calls identified **with 21 providing demonstrator or pilot actions**. Specifically, they relate to **healthcare, manufacturing, energy, agriculture, smart ports and maritime logistics, transport, and smart communities**. This connection between the Cognitive Computing Continuum, development of platforms, architecture and tools, extends beyond the Cluster 4 calls and presents an opportunity for coordinated and combined actions which links the main communities together.

Table 7. Distribution of potential pilots and demonstrators for the Cloud-Edge-IoT Continuum

CLUSTER	BUDGET	Nº CALLS	Nº PROJECTS
1- Health	89.000.000,00 €	3	10
4 - Digital, Industry and Space	24.000.000,00 €	2	4
5 - Climate, Energy and Mobility	188.700.000,00 €	15	25

6 - Food, Bioeconomy, Natural Resources, Agriculture and Environment	40.000.000,00 €	1	1
	341.700.000,00 €	**21**	**39**

The DIGITAL Programme also holds particular relevance across the actions already undertaken in its Work Programme for 2021-2022 and the recently published 2023-2024. Areas related to Energy/Power, Interoperability and Data Sharing are well addressed and **provide market-ready tools, systems, platforms often within specific domains.** The following actions have significant links to the activities of the NGIoT and future Horizon Europe actions should be linked within:

- **Large Scale Pilots for cloud-to-edge based service solutions**: deployment at scale of innovative, sustainable, secure and cross-border cloud-to-edge based services in new and expanded environments.
- **Reference deployments of European cloud-edge services**: simultaneous deployments in real environments to lead fully interoperable next generation edge computing technologies for the seamless integration and seamless interoperability of Industrial IoT Edge with Telco Edge.
- **Data Spaces Support Centre** – Coordinating a shared standards, architectures and governance for Data Spaces.
- **Data Spaces** - development of domain-based Data Spaces in Health, Energy, Manufacturing, Tourism, etc.
- **Procurement of middleware platform SIMPL** – providing the basis for multi-cloud orchestration and interoperability across the cloud computing continuum and Data Spaces.
- **Delivery of Testing and Experimentation Facilities (TEFs)** - accelerating deployment of AI both domain-based and cross-cutting for Edge AI Hardware, to develop, test and experiment AI product prototypes based on advanced low-power computing technologies, custom-designed for their application environment.
- **Marketplace for Federated Cloud-to-Edge Services**: single point of access for trusted services providing brokering and supply of cloud-to-edge services to the public sector and industries.
- **AI-on-Demand Platform** – supporting the reuse and sharing of trustworthy AI solutions that aligns to the European vision for AI and provides a boost to development and wide-scale deployment.
- **AI Act Platform** – database to provide the registration of high-risk AI applications and submission of data for management of compliance with regulatory authorities.

4 POLICY ANALYSIS

4.1 A new age for Digital Policy development

The past decade has been one in which European political leaders have navigated a myriad of societal and economic challenges that have demanded measures that increase Europe's resilience to systemic shocks and ability to compete in a less stable global political environment.

The convergence of health, climate, energy and political crises has required a branch and root transformation of how European businesses and citizens operate and has amplified the need to adjust to the digital and green transitions. Ensuring Europe's digital "sovereignty", understood as supporting technological choice, has become a fundamental tenet of future competitiveness, even underpinning social freedoms.

The pace **of technological development continues to accelerate and policymaking now, more than ever, must seek to be future-proof, taking into account how data and technology usage will evolve in the near and more distant future.** The go-to-market timeline for AI is accelerating. OpenAI's CodeX went from research to commercialization in 12 months. Two months after its launch, its sibling model ChatGPT had gained 100 million users. A slew of (imperfect) AI solutions is widely available now from all hyperscalers, including Microsoft's GitHub Copilot as well as their $1 billion investment in OpenAI, Amazon's CodeWhisperer and Google's Bard.

A foretaste of the impact of technology on civil liberties can be seen in the work currently being conducted by the European Agency for Fundamental Human Rights, "Using AI systems engages a wide range of fundamental rights, regardless of the field of application. These include – but also go beyond – privacy, data protection, non-discrimination and access to justice."[11] In March 2023, an Open Letter to the Future of Life Institute signed by leaders from civil society, academia and technology, including Steve Wozniak, Co-founder of Apple, called on "*on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4. This pause should be public and verifiable, and include all key actors. If such a pause cannot be enacted quickly, governments should step in and institute a moratorium"*.

The role of policy has rarely been of greater importance. **The European Union has a globally prominent role to play, shaping the regulatory landscape that balances the freedoms that lead to innovation with the protection of the rights of citizens and businesses while attempting to provide legal certainty.**

4.2 Non regulatory measures driving NGIoT adoption

Across Europe, policymakers are launching initiatives to update existing regulatory and normative frameworks, adapting them to the all-pervasive digital economy that is shaping society, business, and even politics. Many of them will have a direct impact on the future of the next-generation IoT and the move to the Cloud-Edge-IoT paradigm.

[11] Getting the future right. Artificial intelligence and fundamental rights. FRA. 2020.

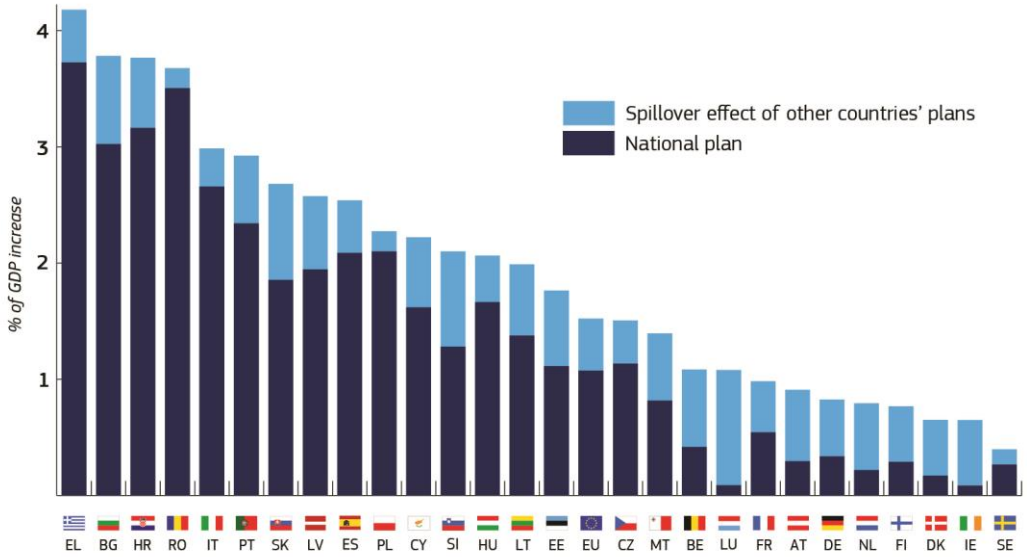


Figure 7. Quantifying Spillovers of Next Generation EU Investment, Discussion Paper July 2021. European Commission.

The deployment of the Recovery and Resilience Fund, a temporary recovery instrument that made available a total of €723.8 billion[12] in loans (€385.8 billion) and grants (€338 billion) to Member States to implement reforms and new initiatives aligned with EU priorities around climate change and the digital transition, has accelerated the review and deployment of policies and instruments that regulate the digital and data economy for consumers/citizens and businesses.

To date, Member States[13] have allocated close to 40% of spending to climate measures and more than 26% on the digital transition, exceeding the respective targets of 37% and 20%, with significant cross-border spillover effects that highlight the financial benefits of pursuing a single digital market (Figure 7, above).

Examples of measures include:

- UNICO R&D (Spain) - The UNICO Framework Plan (Universalisation of Digital Infrastructures for Cohesion) seeks to provide connectivity with the development of digital infrastructures and achieve full territory coverage of fast broadband networks across the territory by 2025. It is the main instrument for the deployment of the Spanish Recovery, Transformation and Resilience Fund Component 15: Digital connectivity, promotion of cybersecurity and deployment of 5G. During its first stage 2021-2022, €249.9 million were invested in financing for the execution of 52 projects to deploy fast broadband infrastructure and stimulate the coordinated research and development into advancing 5G network capabilities for privacy, localisation, and self-healing.
- R&I for the Digital Economy (Slovakia): Slovakia is investing €134 million into the R&I for Digital Economy supporting over 150 projects in the development of sensors and IoT; microelectronics and electronic components, and cloud solutions which will support the competitiveness of Slovak SMEs and research institutions in the market, as well as their

[12] In current prices.

[13] Across 22 recovery and resilience plans approved to the report's date.

readiness to participate in further key strategic HE and IPCEI projects[14].

4.3 Regulatory measures shaping the NGIoT

The full impact of this significant level of investment into the digital economy will be contingent on the effective functioning of the Single Digital Market. In turn, this relies on the implementation of a harmonised regulatory[15] framework that can protect rights and provide guidance and legal certainty to all stakeholders. From this perspective, the most relevant regulations set to shape the NGIoT include:

- Proposal for Data Act {SEC(2022) 81 final}
- Proposal for Cybersecurity Resilience Act {SEC(2022) 321 final}
- Proposal for Artificial Intelligence Act {SEC(2021) 206 final}
- Digital Markets Act {Regulation (EU) 2022/1925}
- Digital Services Act {Regulation (EU) 2022/2065}
- Proposal for Chips Act {SEC(2022) 46 final}
- Proposal for Data Governance Act {SEC(2022) 868 final}

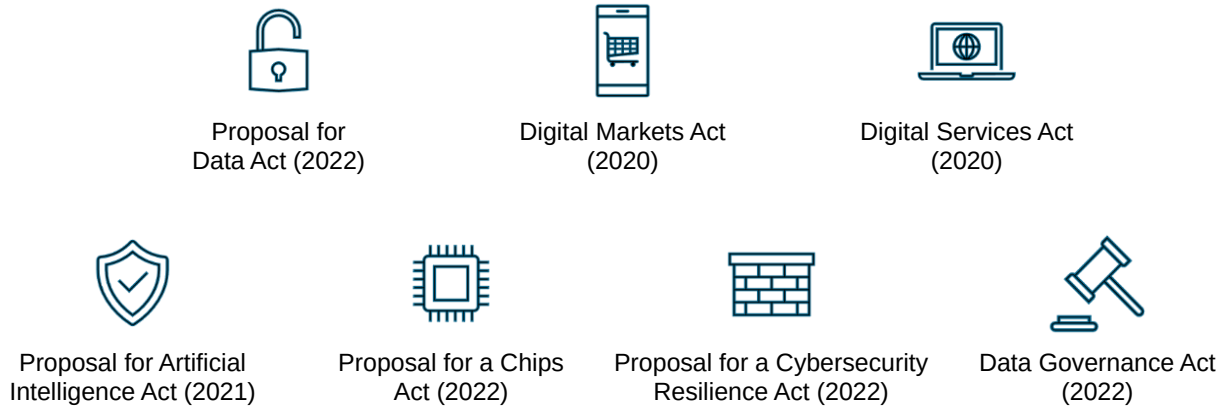


Figure 8. Main regulations that are likely to have a direct impact on the NG-IoT

Each of these regulations will have a different degree of impact on the technology community, with the **Data Act expected to hold the most direct and significant impact on how solutions are designed, developed, and deployed**, and how its provisions also open up new business opportunities. Each of these regulations also confers a distinct set of rights and obligations on the stakeholders in the digital ecosystem, seeking to clarify what can and cannot be done with data in a range of settings.

This report will place the greatest emphasis will on the analysis of the **Data Act** approved by the European Parliament on 14th March 2023, and provide an update on the debate surrounding the **Proposal for Cybersecurity and Resilience Act,** and the **Proposal for the Artificial Intelligence Act**. Finally, it will provide a summary of the **Digital Service Act Package**.

[14] Recovery Plan (2021) Government Office of the Slovak Republic

[15] A "regulation" is a directly applicable form of EU law, which has binding legal force in all member states. National governments do not have to take action to implement EU regulations. A "directive" is a legislative act setting a goal to be achieved by all EU countries, but leaving the method to each member state.

4.4 The Data Act

4.4.1 Purpose and scope

The Data Act is the first industrial data regulation in the European Union. It was approved by the European Parliament on March 14th 2023[16] and is now pending approval by the Council. Its focus is on the rights and obligations around the sharing of non-personal data generated through the use of a connected product or a related service. It addresses the need to release the economic value of data, clarifying rights and obligations, addressed imbalances in data-sharing agreements and generally improve data access and use.

Its central tenet is that data is generated through the actions of a designer or manufacturer of a connected product and its user. Consequently, **manufacturers of connected products and related products** must design their products and services in a way that ensures that the **data it collects or generates is made available to the user**, or a third party designated by them in a transparent, fair, reasonable and non-discriminatory manner.

It is of critical importance to companies operating in the Cloud to Edge continuum, as it recognises the value of the data collected and processed in the course of the use of a connected product, **removing obstacles to data portability of that data** and generally aiming to enhance the **interoperability of data and data sharing** mechanisms and services.

The Act does not purport to modify existing obligations relating to the protection of personal data and the right to privacy and confidentiality of communications, but rather acts on adapting general principles of contract law.

The Act also recognises that its provisions will be effective only in so far as businesses understand how they can be leveraged to support business goals. It has a provision to support data literacy but is vague on who has the obligation to support data literacy or the mode in which this obligation can be discharged: " *Member States shall promote measures and tools for the development of data literacy, across sectors and taking into account the different needs of groups of users, consumers and businesses, including through education and training, skilling and reskilling programmes and while ensuring a proper gender and age balance, in view of allowing a fair data society and market*."

There is also a specific call for the Act to be followed by sectoral legislation, for instance, to improve data sharing in the Mobility sector, or to govern the right of suppliers to access data from their own smart components for issues such as quality monitoring, product development or safety improvements.

Stakeholders

Business users, consumers, data holders (device manufacturers or service providers), data processing service providers, third-party data processors (supplier to user and supplier to manufacturer or service provider), and public bodies.

4.4.2 Main exclusions and limitations

Types of data

- Data generated by prototypes.

[16] P9_TA(2023)0069

- Data inferred or derived from usage of the product or service.
- Data generated from devices primarily designed to display, play, transmit or record content, such as mobile phones and tablets.
- Personal data; must be requested through a data controller or subject as under GDPR.

Data users

Where the data user is not a data subject, any personal data can only be shared if there is a valid legal basis. Gatekeepers, designated as such under the Digital Markets Act (such as large-scale platforms, including cloud computing platforms) do not have the rights to access or process the data within this regulation.

Data holders

The data holders themselves may not use the data generated through the use of a connected product or service to gather insights on the user that might undermine their competitive position or to develop products and services that might enter into direct competition with those of the data user.

SMEs

There are specific exclusions for SMEs, who are not required to comply with design obligations except where they are acting as sub-contractors for the design and manufacture of a product. They are also exempt from complying with data requests from public authorities.

4.4.3 Implications for the NGIoT

The Act applies to connected products and services that generate data through user interaction. It is based on the premise that, beyond pseudonymisation and encryption, the state of the art allows for technical and organisational measures to protect data, by allowing information to be derived from the data sets without transferring the data itself. The techniques range from providing data virtualisation or Application Programming Interfaces (APIs) to metadata masking.

Access to data by design and by default

Connected products and their related services must be **designed and manufactured or provided in a way that data generated through use is accessible by the user by default**, easily, securely and, where relevant and appropriate, directly.

Data holders **cannot offer preferential conditions for access to data, such as partners or linked companies**. Any compensation that might be agreed upon between the data holder and the data recipient must be reasonable. In the case of SMEs, the compensation cannot exceed the cost of making the data available.

There are also specific provisions under Article 13 that protect SMEs from unfair contractual terms that have been unilaterally imposed, enabling them to seek remedies for the breach or termination of data-related obligations. An unfair term is one that "*grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing*."

Provision of data to the public sector in cases of exceptional need

Data holders are required to **provide data to public sector bodies and agencies to respond, prevent or recover from public emergencies**, and to fulfil specific tasks that are in the public interest explicitly provided by law, unless this data can be obtained through alternative means, including market purchase.

The Act does not give *carte blanche* to the public sector in these instances but requires proportionality in terms of the granularity, volume and frequency of access to the data. The requests also must respect the legitimate aims of the data holder, including trade secrets. The public sector organisation requesting the data may not then make this data available for reuse.

Data must be provided free of charge in the case of responding to an emergency, but reasonable costs may be recovered in the other cases.

SMEs are exempt from this obligation.

Transparency on data generation

The user must also be provided with information regarding the data generated through the use of a connected product or service in a clear and comprehensible format, before it is bought, rented or leased. This information includes:

- The nature and volume of the data likely to be generated by the use of the product or related service.
- Whether the data is likely to be generated continuously and in real-time.
- How the user may access the data.
- Whether the supplier or service provider intends to use the data itself or allow a third party to use the data and, if so, the purpose for which it will be used.
- Whether the seller, renter or lessor is the data holder and, if not, the identity and address of the data holder.
- The means of communication which enable the user to contact the data holder quickly and efficiently.
- How the user can request that the data be shared with a third party.
- The user's right to lodge a complaint with the competent authority.

Effectively enabling portability

When requested by a user, the data holder must make the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.

Virtual assistants

The Act specifically includes data arising from the use of virtual assistants, (such as Alexa or Google Assistant) that process user demands to provide access to their own or third-party services. The obligations are limited to the data generated through interaction with the user.

Increasing the competitiveness of the Cloud to Edge market

Users of data processing services may find themselves tied to existing data processing services because of a range of practical difficulties in transferring their data to a new provider. These difficulties limit choice and act as a barrier to competition in the data processing market. The Act has several provisions that seek to address these barriers by requiring data processing service providers to:

- Include contractual clauses allowing the customer to switch to another provider or to port all data, applications and digital assets to an on-premise system and facilitate and complete the process within 30 days where technically feasible.
- Remove commercial, technical, contractual and organisational obstacles to effective

switching.

Certain data processors also offer scalable infrastructure as a service (IaaS), essentially acting as virtualised computing resources, including as virtual machines (VMs) or containers, along with storage and networking capabilities, that can be used to build and deploy applications in the cloud. In these cases, the service provider must ensure that their customers enjoy **functional equivalence** in the use of the new service.

Non-IaaS providers must also:

- Provide public open interfaces free of charge.
- Ensure compatibility with open interoperability specifications or European standards for interoperability, where these exist or provide the data in a structured commonly used and machine-readable format.

Measures to ensure Interoperability

Certain measures apply very specifically to operators of data spaces who are required to facilitate interoperability of data, data sharing mechanisms and services through:

- The appropriate description of dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty.
- Data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, which must be described in a publicly available and consistent manner.
- The technical means to access the data (e.g. APIs) and terms of use so data can be accessed and transmitted automatically in a machine-readable format, continuously or in real-time.
- The means to enable the interoperability of smart contracts within their services and activities shall be provided.

In terms of the specifications and European standards themselves, they are required to be performance oriented and to enhance the portability of digital assets between different data processing services (such as descriptive or predictive analytics) that cover the same service type (such as data analysis service).

They will also address:

- Cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability.
- Cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability.
- Cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.

Understanding and applying these standards, which are to be published in a **central Union standards repository** as they are developed, will be a **critical component of the NGIoT.**

Smart contracts

Vendors of applications that use smart contracts must ensure they are **robust,** can be **safely terminated/interrupted,** provide measures to **archive data and keep records** that enable **auditability** and operate rigorous control mechanisms at governance and smart contract layers.

Vendors must perform conformity assessments and issue an EU declaration of conformity.

Conformity will be presumed if the vendor adopts harmonised standards and publishes them in the Official Journal of the European Union.

Protecting intellectual property

Data resulting from a software process that generates derivative data is excluded, as is proprietary data and IPR belonging to the data holder. This will be particularly relevant for image recognition, computer vision algorithms as they analyse images or to identify and extract specific features or patterns, and then generate derivative data based on those features or patterns. Similar to NLP algorithms that may analyse text to extract sentiment. The sentiment analysis should be considered derivative and therefore outside the scope of the Data Act.

The data holder's trade secrets must be protected, particularly with regard to enabling third-party access to the data at the user's behest. In this case, the agreement between the data holder and the third party must specifically identify the data as a trade secret.

Voluntary model contractual terms on access to and use of data

Final provisions include the Commission's obligation to "*develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations*".

4.5 Proposal for a Cyber Resilience Act (CRA)

4.5.1 Purpose and scope

The Proposal for a Cyber Resilience Act (CRA) was published by the European Commission on 15 September 2022. Its main objective is to establish a set of **common cybersecurity standards for connected devices and services**, safeguarding consumers and market operators against cyber incidents.

The CRA comprises a collection of regulations designed to incorporate digital security in Europe, and it also includes two guidelines. The first guideline is on networks and information systems (NIS), seeking to enhance the cybersecurity capabilities of member states through information sharing. The second guideline is the Cybersecurity Act, which came into effect in 2021 and outlines the duties of the European cybersecurity watchdog, ENISA. EU ministers will meet on 2 June 2023 to discuss further changes to the proposal.

Stakeholders

Device manufacturers, importers and distributors; software providers as well as chip manufacturers; local authorities for cooperation and enforcement (still to be confirmed); European authorities: European Union Agency for Cybersecurity (ENISA) and users (consumers).

Main Exclusions

The proposed regulation will not apply to medical devices for human use, accessories for such devices, or products with digital elements that have been certified in accordance with high uniform level of civil aviation safety. Software as a Service (SaaS) is also out of scope except where such SaaS enables remote data processing solutions, as is open-source software developed or supplied non-commercially.

4.5.2 Implications for the NGIoT

Increase in security throughout the NGIoT ecosystem

The increase of security throughout IoT ecosystem is an **essential step towards the increase AI Trustworthiness**, one of the strategic objectives derived from the SRIA agendas analysed in section 3.1 Summary of relevant Strategic Research and Innovation Agendas.

The CRA Act encourages the **creation of a software bill of materials (SBOM),** which will help to provide transparency in exercising rights in the future. This was first promoted by the US National Telecommunications and Information Administration in 2018 in response to the need for greater visibility and transparency into software supply chains, driven by the increasing complexity of software development, the growing reliance on open-source software, and the rise of software vulnerabilities and supply chain attacks.

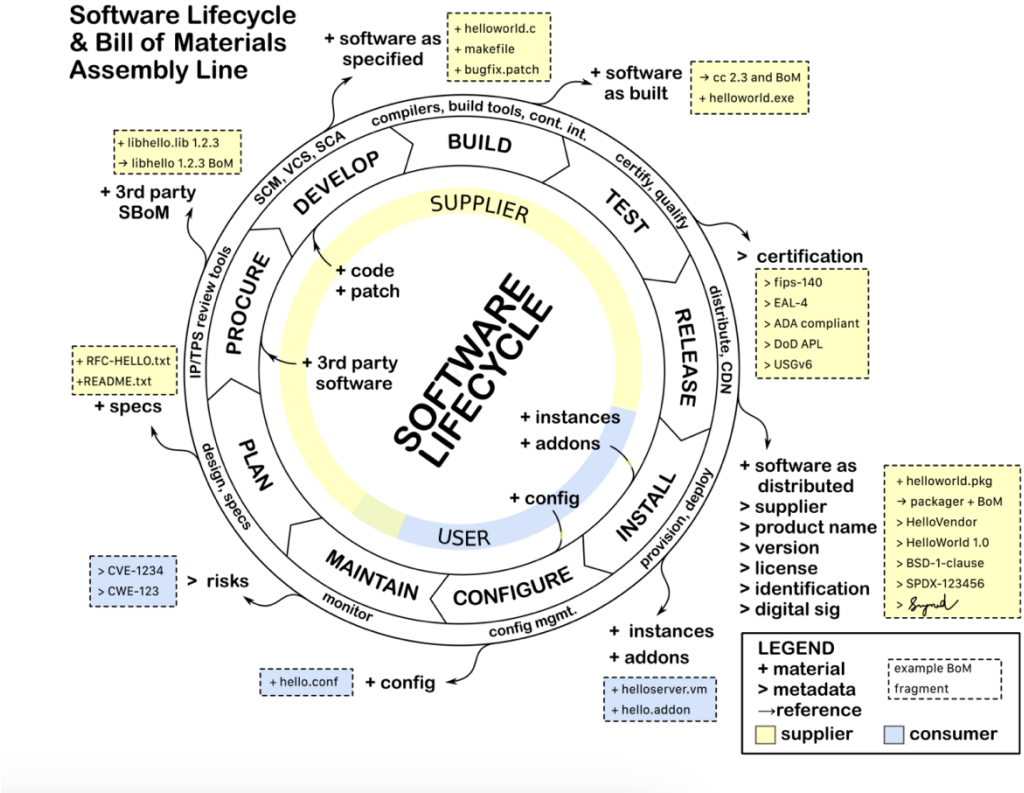


Figure 9. SBOM in the software cycle. Survey of Existing SBOM Formats and Standards (2021) NTIA.

Scope complexities

According to Industry associations involved within the NGIoT ecosystem, the current scope of the CRA may make specific stakeholders accountable or responsible for consequences that can take place beyond their intervention in the value chain[17]. That specifically applies to the applicability of compulsory criteria of trust, confidentiality, and integrity of stored and transmitted data on to software developers and chips manufacturers. Regardless the initial design of, for example, a chip, the device maker may choose not to make use the security features of the chip and/or the

[17] AIOTI Views on the Cyber Resilience Act, 2023

system software or use them in a way that is different from the supplier's intent.

Potential perverse incentives

The current proposal imposes an obligation on manufacturers to deliver products without any known exploitable vulnerability. This may perversely generate incentives for less testing for vulnerabilities as the Act only penalises the release of products with vulnerabilities that had been previously tested.

Additionally, there are several concerns around reporting, as disclosing an "actively exploited vulnerability"[18] may prompt manufacturers to disclose an exploitation that could potentially affect the product before a fix/patch is available. This is contrary to existing Coordinated Vulnerability Disclosure (CVD) practices and standards that aim to safeguard customers. Making public information about an unaddressed vulnerability may result in more cyber-attacks.

4.6 Proposal for an Artificial Intelligence Act

4.6.1 Purpose and scope

Description

The AI Act aims to provide clarity around what can and cannot be done with artificial intelligence in the European Union. It **establishes harmonised rules for the placing and using AI on the market, and prohibits certain practices**. It outlines specific requirements for high-risk AI systems and obligations for operators of such systems.

It also provides harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content. Finally, it set out the rules on market monitoring and surveillance.

Stakeholders

Providers of AI systems in the EU; users of AI systems located within the Union; providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union; subjects of AI systems.

It is worth noting that distributors, importers, users or other third parties are considered to be providers and are subject to the Act if:

- They place on the market or put into service a high-risk AI system under their name or trademark.
- They modify the intended purpose of a high-risk AI system already placed on the market or put into service.
- They make a substantial modification to the high-risk AI system.

Main exclusions

AI systems developed or used exclusively for military purposes; AI used by public authorities in a third country or international organisations in the framework of international agreements or for law enforcement and judicial cooperation with the Union or with one or more Member States.

[18] P.18 2022/0272 (COD)

4.6.2 Implications for the NGIoT

There have been several iterations on the initial proposal for an AI Act with the main discussion centred along five axes[19]:

General scope and purpose

The categorisation of "AI systems" is central to the Act, imposing varying degrees of regulation according **to three risk categories**:

- **Unacceptable risk:** AI systems considered a clear threat to the safety, livelihoods and rights of people will be banned, from social scoring by governments to toys using voice assistance that encourages dangerous behaviour.
- **High-risk applications**: these applications (such as critical infrastructures (e.g. transport), that could put the life and health of citizens at risk, or safety components of products (e.g. AI application in robot-assisted surgery), or essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan) must apply a range of measures to ensure compliance.
- **Non-high-risk** are largely left unregulated with provision for voluntary codes of conduct to be drawn up by individual providers of AI systems or by representative organisations, involving stakeholders.

There is currently a call to clarify the responsibility of manufacturers and developers of high-risk AI systems.

High-risk AI obligations

The Act requires High-risk AI systems to be "*designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately*". They must also complete a conformity assessment. Other requirements include:

- Ensuring the high quality of the datasets feeding the system to minimise risks and discriminatory outcomes.
- Logging activity to ensure traceability of results.
- Providing detailed documentation on the AI system and its purpose for authorities to assess its compliance.
- Providing clear and adequate information to the user.
- Ensuring appropriate human oversight measures to minimise risk.
- Applying high levels of robustness, security and accuracy.
- Implementing adequate risk assessment and mitigation systems.

High-risk AI systems must also undergo a new conformity assessment procedure whenever they are "*substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current user*".

Distributors are subject to strict obligations as they are required to (i) verify that the high-risk AI system has the CE conformity marking, (ii) that it has the required documentation and instructions of use, and (iii) that the provider and the importer of the system, as applicable, have complied

[19] Committee on Legal Affairs, 12.9.2022

with the obligations set out in the Act.

Conformity assessment and harmonized standards

The Council expresses the industry's concerns about potential conflicts with current conformity assessment regulations and the absence of established standards for ensuring compliance. The proposed three-year transitional period is deemed inadequate for adequate implementation, and there is a shortage of designated organisations for assessing the conformity of AI systems. Consequently, users and providers of high-risk AI systems are recommended to monitor the situation closely and include protective provisions in their contractual agreements with AI system providers and developers.

Regulatory sandboxes

A "sandbox" provision is included in the AI Act, which aims to establish controlled environments where developers can create, train, test, and validate innovative AI systems under realistic conditions. Most stakeholders agree these controlled environments crucial for fostering innovation, and that they will offer developers greater certainty and cost savings. On this matter, while the Parliament It is suggested some form changes that do not affect the scope of the sandbox according to the proposed act the Council suggests that solutions tested in sandboxes should have limited or no liability at the Member State level, which will result in a more flexible approach overall. This provision is specifically intended to assist small and medium-sized enterprises (SMEs) and start-ups, which are the main catalysts of innovation in the AI field.

Supervision and coordination

The AI Act provides for enforcement through a governance system at Member State level that builds on existing structures, and a cooperation mechanism at Union level through a European Artificial Intelligence Board. The Board's role is to guide the Commission in order to:

- Contribute to the effective cooperation of the national supervisory authorities and the Commission.
- Co-ordinate and contribute to guidance and analysis by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market.
- Assist the national supervisory authorities and the Commission in ensuring consistency in the application of the Act.

The Board will be composed of the national supervisory authorities, represented by the head or equivalent high-level, and the European Data Protection Supervisor. There are calls, however, for the AI Board to have greater autonomy to involve relevant stakeholders in key issues and guarantee the implementation of the Act throughout a serving body and platform.

4.7 The Digital Services Act Package

4.7.1 Scope, Purpose, and current status

The Digital Services Act Package is a legal framework consisting of the Digital Services Act (DSA) and the Digital Markets Act (DMA) that aims to provide a safer digital space for users and a level playing field for businesses. The **DSA sets out rules for online intermediaries and platforms, including online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms**, to protect the fundamental rights of all users of digital services. Online platforms will be required to take measures to prevent the dissemination of illegal content and products, to provide transparency to users on how content is moderated,

and to ensure that users are informed about targeted advertising. The **DMA, on the other hand, governs gatekeeper online platforms that have a systemic role in the internal market and function as chokepoints between businesses and consumers** for important digital services.

The DSA was published the Official Journal on October 27, 2022, and went into effect on November 16 of the same year. It will have a direct impact throughout the European Union and will be enforceable either fifteen months after its entry into force or from January 1, 2024, whichever comes later.

The Digital Markets Act (DMA) was officially published on October 12, 2022, and became effective on November 1, 2022. Companies are required to provide the Commission with their user numbers by July 3, 2023, so that the Commission can designate "gatekeepers" before September 6. After that, gatekeepers will have until March 2024 to comply with the obligations set forth in the DMA.

Stakeholders

The DSA affects Intermediary service providers such as social media platforms, search engines, e-commerce marketplaces, and online booking platforms. It also affects recipients of intermediary services such as online sellers and buyers.

The DMA stakeholders include the companies or platforms such as gatekeeper, that are platforms that have significant impact on the internal market, operate a core platform service which serves as an important gateway for business users to reach end-users, and enjoy an entrenched and durable position in the market. Additionally, consumers and users of these platforms are also stakeholders, as the DMA aims to improve their rights and protections. National regulators and competition authorities. Finally, industry associations and civil society groups are stakeholders that may provide input and feedback on the implementation and effectiveness of the DMA.

Main exclusions

The DSA excludes services that are known as “mere conduit”, “caching” and “hosting” services; these being internet service providers that provide basic transmission services and do not modify the content of the information transmitted, providers that temporarily store information for the sole purpose of more efficient transmission, and providers that store content at the request of their users. It also excludes micro and small enterprises.

On the other hand, the DMA excludes electronic communications networks and electronic communications services as well as device manufacturers and software developers.

4.7.2 Implications for the NGIoT

It is likely that the package will have an impact on NGIoT, particularly to companies that may become designated as "gatekeepers" under the Digital Markets Act. These companies may face additional regulatory obligations and restrictions, which could have implications for their ability to innovate and develop new IoT technologies. The **limit on current market-established gatekeepers to maintain their dominant position in the market can also be assumed to promote innovation and competition amongst smaller players and allow cloud-edge platforms to develop further**.

On the other hand, the DSA includes provisions that aim to promote online safety and security, including measures to combat illegal content unfair practices. These provisions may have a positive impact on the IoT research and innovation environment by promoting trust and confidence in online platforms, which are increasingly important for the successful deployment of IoT technologies as they address AI Trustworthiness.

Additionally, the DSA includes provisions to address issues related to liability and accountability

for online intermediaries, which could help to clarify legal obligations and reduce legal uncertainty within the NGIoT ecosystem.

Finally, on more immediate implications companies have until March 2024 to ensure that they follow the obligations of the DMA, while platforms with more than 45 million users will have to comply with the obligations of the DSA by 1 January 2024 while during the course of 2023 companies and platforms will be required to inform on their total number of users.

5 SUMMARISING OF IMPACT ON THE NG-IOT

As can be seen from the analysis of the SRIAs, the NG-IoT is diverse in terms of stakeholders, domains, technologies and applications. While an exhaustive look at each of the acts and proposed regulations is outside the scope of this report, it may be useful to briefly summarise:

- The most salient rights and obligations that may have an impact on the organisations that will form part of the NG-IoT.
- Key figures across the new regulatory framework.
- The cost of non-compliance.

5.1 Rights and obligations

The table below summarises:

- The rights that will be conferred by the new proposals and that may give access to interesting resources and capabilities.
- The obligations that will come into force and that should be taken into account at the earliest possible stage in the process of designing and testing the NG-IoT architectures.

Purpose	Main obligations
Data Act	
Ensuring that the user is able to make use of their generated data and stimulate innovation based data and deliver choice and autonomy.	Data Holders • Provide users with timely access to data resulting from the use of the product or related service. • Make data available under fair, reasonable and non-discriminate terms in a transparent manner. • Make the data available to the same level as available to themselves (completeness, accuracy, reliability, up-to-date). • Make data available to public bodies under an established exceptional need. • Provide SMEs with the data at cost price for making the data available. • Provide information of how data can be accessed within contract, leasing or purchase agreements. • Provide description of the data generated, who will process and use it within contract, leasing or purchase agreements. • Provide a breakdown of costs of supply of data when charging data user. They must not • Impose unfair contractual terms on SMEs. • Use any data from use of product or service to derive economic status or production methods to undermine the commercial position of the user. i.e. use own data against them commercially either directly or indirectly.

To prevent vendor lock-in with cloud and edge providers due to technical incapacity for switching limiting market growth and innovation.	Data Processing Service Providers • Port all digital assets of the customers – data, applications, virtual machines, etc. • Provide necessary support for successful completion switching. • Ensure, that where applications or similar cannot be ported, that the customer achieves functional equivalence of the new service. • Prevent access to systems through robust cybersecurity practices. • Provide open interfaces for data processing services that are not tied to their infrastructure. • Ensure compatibility with defined interoperability standard or provide the data in a structured, commonly used format.
Cybersecurity and Resilience Act	
To enhance the security and resilience of digital products in the European Union by imposing essential security requirements on connected devices. The law is a response to the ever-increasing threat posed by cyber criminals, who continuously innovate and evolve their attack techniques.	• Manufacturers and developers of products with digital elements must meet specific essential cybersecurity requirements before their products can be made available on the market. • Manufacturers must factor cybersecurity in the design and development of the products with digital elements, and must provide security updates and support for a reasonable period of time. • Manufacturers must be transparent about cybersecurity aspects that need to be made known to customers and must provide up-to-date information about the end-of-life of the products and the security support provided. • Economic operators, starting from manufacturers, up to distributors and importers, must comply with obligations for the placing on the market of products with digital elements, as adequate for their role and responsibilities on the supply chain. • Manufacturers would undergo a process of conformity assessment to demonstrate whether the specified requirements relating to a product have been fulfilled, which could be done via self-assessment or a third-party conformity assessment, depending on the criticality of the product in question. • In case of non-compliance, market surveillance authorities could require operators to bring the non-compliance to an end and eliminate the risk, to prohibit or restrict the making available of a product on the market, or to order that the product is withdrawn or recalled, and could fine companies that don't adhere to the rules.
Artificial Intelligence Act:	
Proposes a single future-proof definition of AI and sets harmonised	Prohibited artificial intelligence practices include systems or services that, inter alia: • Use subliminal techniques to materially distort a person's

rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach	behaviour in a manner that could cause physical or psychological harm. • Evaluate or classify of the trustworthiness of natural persons based on their social behaviour or known or predicted personal or personality characteristics, that can lead to detrimental or unfavourable treatment of people or groups in social contexts which are unrelated to the contexts in which the data was originally generated or collected or is unjustified or disproportionate to their social behaviour or its gravity. • Use of real-time remote biometric identification system other than in the instances expressly allowed. Amongst other obligations, high-risk AI systems[20] require establishing, implementing and documenting a risk management system that: • Identifies and analyses the known and foreseeable risks associated with each high-risk AI system. • Estimates and evaluates the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse. • Evaluates other possibly arising risks based on the analysis of data gathered from the post-market monitoring system (Art 61). • Adopts suitable risk management measures in accordance with the provisions of the following paragraphs. In addition: • In eliminating or reducing risks related to the use of the high-risk AI system, the user's technical knowledge, experience, education, training and the environment in which the system is intended to be used must be taken into account. • The tests should enable the most appropriate risk management measures to be identified, ensuring the system's consistent performance and compliance. • The tests must be performed pre-market placement against pre-defined metrics, and suitable to achieve the intended purpose of the AI system but do not need to go beyond this. In relation to the data and data governance, high-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 of Art. 10. Personal data may be processed to ensure bias monitoring provided state of the art security and privacy-preserving measures are introduced.

[20] Defined in Art. 6

	Other important provisions include: • The obligation to draw up technical documentation before the system is placed on the market. • Automatic recording of events (´logs´) while the AI system is operating. • Ensuring sufficient transparency. • Incorporating human-machine interface tools to enable natural persons to oversee the AI system when it is in use. • Providers must affix the CE marking to indicate conformity. It also provides for voluntary Codes of Conduct that will include requirements in relation to environmental sustainability, accessibility, stakeholder participation in design and development, diversity in development teams etc.
Digital Services Act Package	
Digital Markets Act (DMA)	
To end unfair restrictions imposed by large-scale platforms, including cloud computing platforms, to reduce lock-in effects and increase innovation.	Inter alia[21], Gatekeepers must: • Provide effective portability of data. • Provide business users or third parties authorised by them with effective, high-quality, real time, continuous access to aggregated or non-aggregated data. • Provide access to personal data only when this is directly connected to the use. • Allow businesses to offer services outside the core platform on different terms. • Impose the use of the gatekeeper's own identification services own platform on business service users own offering. • Provide advertisers and publishers with data on the performance of ads. They must not: • Technically restrict the ability of users to switch to other applications and services using the OS of the gatekeeper. • Combine personal data sourced from the core platform services with any other personal data from services offered by them or data from third-party services. • Automatically opt in end-users to additional services offered by them. Rank their own services above those of other business user.

[21] Key points. Full obligations are set out in articles 5 and 6 of the proposed regulation.

Digital Services Act (DSA)	
Sets out obligations on intermediary information society services to ensure the proper functioning of the internal market and a safe, predictable and trusted online environment in which the fundamental rights enshrined in the Charter are duly protected	Intermediary service providers, including online platforms, must set up single points of contact in the EU. Due diligence obligations for online safety and transparency include: • Provide information on any restrictions on the use of their service, including information on any "…policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review." • Annual reports on content moderation. • Mechanisms to allow "any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content". • Prompt notification of suspicion of serious criminal offence involving threat to life or safety of persons. • Provision of reasons for any detection, identification, removal or disabling of access to content. • Establishment of systems to promptly act on notices submitted by trusted flaggers. • Obligation to collect information on traders offering products or services to EU consumers and to provide an online interface that facilitates compliance with pre-contractual obligations and product safety information • Transparency on advertising. Additional obligations are placed on very large online platforms which serve more that 45 million monthly active recipients in the Union.

5.2 Defining key roles (relevant to NGIoT)

Regulation	Key Figure	Definition
Data Act	Data Holder	The manufacturer of a connected product or related service provider who receives the data generated from the use of the product or service that is put into the Single Market.
	Data Processing Service Provider	Providers of on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature which includes cloud or edge computing platform providers but not content platform providers.
Cybersecurity and Resilience Act	Economic Operators	Manufacturers, importers, and distributors based on the reference provisions foreseen in Decision

		768/2008/EC[22] this includes chip manufacturers, software suppliers, and OS/Software platform vendors along with all stages of the value chain.
Artificial Intelligence Act	AI providers	Providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country.
	High-risk AI systems	Where the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II; or the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II; or any system in Annex III.
Digital Markets Act	Gatekeeper	A provider of core platform services that has a significant impact on the internal market, operates a core platform service which serves as an important gateway for business users to reach end users and enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future.
Digital Services Act	Digital Services Coordinator	Member States shall designate one of the competent authorities as their Digital Services Coordinator, responsible for all matters relating to application and enforcement of this Regulation in that Member State, unless certain specific tasks or sectors have been assigned to other competent authorities.
	Trusted Flagger	Status awarded by the Digital Services Coordinators to entities that: (a) are expert and competent in detecting, identifying and notifying illegal content; (b) represents collective interests and is independent from any online platform; (c) carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.

5.3 The cost of non-compliance

The architectures, applications and data that stem from NG-IoT must be developed in a way that is compliant, as well as competitive. The table below provides a high-level of summary of the of the principal penalties for breach of the provisions in the regulations:

Instrument	Principal penalties for non-compliance

[22] Decision on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC

Data Act	• Fines up to 20 000 000 EUR, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. • Fines of up to 50 000 EUR per infringement and up to a total of 500 000 EUR per year for non-compliance with public bodies requests.
Cyber Resilience Act	• Includes a series of penalties — corresponding to the seriousness of the infringement — which, in the event of a breach of the essential cybersecurity requirements for these products, can amount to EUR 15 million or 2,5 % of turnover for the preceding financial year. • It must be ensured that they are fully operational in practice, not least in order to prevent the Cyber Resilience Act adding to the existing administrative burden and thus penalising manufacturers that will have to comply with a number of additional certification requirements to be able to continue to operate on the market.
Artificial Intelligence Act	Market surveillance authorities are responsible for supervising and enforcing the rights and obligations. Where it has sufficient reason to believe an AI system presents a risk to health and safety or fundamental rights, it must carry out an evaluation. Where non-compliance has been established, the operator must take corrective action throughout the Union, which may involve withdrawal or recall. Penalties must be effective, proportionate and dissuasive, taking into account the interests of small-scale providers and startups and their viability: • Non-compliance with Art 5 & 10: 30 M EUR or 6% of total worldwide turnover. • Non-compliance with other provisions: 20 M EUR or 4% of total worldwide turnover. • Incorrect or misleading information: 10M EUR or 2% of total worldwide turnover. Fines may also be imposed on Union institutions, agencies and bodies (art. 72).
Digital Markets Act	• Fines of up to 10% of the company's total worldwide annual turnover, or up to 20% in the event of repeated infringements. • Periodic penalty payments of up to 5% of the average daily turnover. Additional proportionate penalties may be imposed after a market investigation.
Digital Services Act	• Fines imposed on very large platforms found to be in breach of the regulation vary between 1-6% of total turnover in the preceding year.

6 CONCLUSIONS

6.1 The onward progress of the NGIoT

6.1.1 The era of federation and heterogeneity

The advancement of the **NGIoT Initiative has been a significant contributor towards the federation of devices, systems, and intelligence. The architectures, microservices, tools and use cases that have demonstrated the scaled deployment of collaborative and contextual IoT** is reflected in the overarching theme of federation across all SRIAs.

The demand for interoperability at all levels and the deployment across heterogenous devices and systems heralds the arrival of the Cloud-Edge-IoT continuum and demand for distributed computing across networks and cloud environments. **The flexibility provided is to answer challenges faced by businesses, linked to data sovereignty, control and management, efficiency, scalability of systems and guarantee of service with inevitable greater levels automation**.

All **SRIAs confirm the vision and demand for the continuum**, building on the NGIoT, they seek to address from different aspects the necessary technical challenges from new, adaptive components and chips through to AI solutions to provide the autonomous management of whole systems at scale and ensuring the interoperability of data models. The advancement of federated learning and distributed intelligence is a top priority as is privacy and trust.

With the **increased risk of the integration on a logarithmic scale of devices, edge nodes, 5G networks and shared or distributed models,** secure interfaces are to be ensured and the construction of active and proactive defences, including common standards, platforms, and software components. **Solutions and platforms must also consider how physical devices and data models do not become threats and their legacy integration** is part of the systems to be built, ensuring the longevity of service to the working life of components.

6.1.2 Developing trust and resilience

The **Cloud-Edge-IoT paradigm, while providing promise of lower costs, reduced emissions through orchestrated and distributed processing and the scaling of intelligence, significantly increases the complexity and dynamic nature of the computing systems**.

The management of such complexity requires AI to support the development and execution of applications which comply and adapt to environmental and regulatory constraints and deliver the resilience for the infrastructure on which it is based. The application of robustness and self-organization in response to incidents and ensure the continuity of service is a fundamental of the federated future. **Without confidence of resource availability and assured redundancy, edge computing and distributed systems will remain solely in a research environment**. Resilience and reliability of systems and associated security needs further development to deliver an industry ready, continuous deployment environment.

Matched to this is the requirement for the platforms and tools to support development on federated resources and with virtual devices and digital twins**. Investment is required to create the interfaces for developers and reduce the skills demand to be able to build and run their applications and access autonomous management and orchestration.**

The human relationship with AI and the **collaborative engagement with decision-making and devices like robots is an ongoing challenge**. Human operators must have the confidence and awareness of consequences when applying or responding to AI generated prompts. This must also **consider the multi-modality of human-device interfaces, through haptics, XR and**

similar.

How models are built and managed is just as important to how they are deployed, hybrid intelligence is an avenue for abstracting human knowledge and expertise and ensure the applicability of outputs but also for acceptance. Added to this is the emphasis on **providing data for AI that supports ethical and secure model training which reduces bias and improves performance,** and also provides for where there is limited or inconsistent data available.

6.1.3 Stimulating the competition to the top

Distributed intelligence and federated learning is the guiding demand from the community which is being addressed in existing policy instruments. Funded projects aim to provide the components, architectures, tools and platforms for realising the mass adoption of distributed intelligence. Cross-cutting is the **need to ensure the performance and creation of best in class by driving benchmarks across federated systems for efficiency, frugal use of data, security, privacy and accuracy.**

As evidenced both within the SRIAs and in the calls of Horizon Europe, there are already target use cases and market contexts where the computing continuum may provide an advantage over existing cloud-based or closed system solutions. The challenge remains to both **clearly define and prove the business case behind the solutions under development** with billions of euros of investment.

This is indirectly referenced across all areas; **market dynamics require the advances in power, chip production, energy efficiency, developed HPC assets,** etc. which are among the topics identified. **Continued work needs to advance on the market demand and the preparation of the industry adopters who need to make the case for investing in edge computing** and the active participation in the ecosystems being generated through off-the-shelf models, digital twins, and Data Spaces. **Skills and talent are wholly underrepresented across the board**, and must be addressed in the context of commercial feasibility, it is a complex problem that requires whole ecosystem mobilisation and the engagement of new communities of education and training providers previously seen as further ‘downstream’ of tech development.

The emergence of a Cloud-Edge-IoT continuum, also presents new opportunities for new business models. Through the virtualisation of assets, it is feasible to explore new forms of revenue generation and asset sharing, already under exploration through the delivery of micropayments and the tokenisation of renewable energy. The implementation of the NGIoT across B2C environments in use cases such as in smart building, grid flexibility and EV charging involves a change in consumer behaviour, even a relinquishing of control. **OEMs and service providers must be engaged to define not just new business models but the behavioural economics behind the deployment in society** of the CEI.

6.1.4 Convergence across the digital sphere

The Next Generation IoT is now the Cloud-Edge-IoT computing continuum, there is such evidence of convergence that the themes and challenges addressed under the NGIoT are now underpinning the whole scale digital transformation of large and important value chains such as energy, manufacturing, or even aerospace. The demand for good data, good intelligence and effective investment in digital is driving the need for federated and trustworthy systems, new devices and new platforms. **The eventual success, in part, of the guiding twin strategic policies of Europe, Digital Decade and the Green Deal rely on the development of the Cloud-Edge-IoT.**

The confluence of data, intelligence and diverse processing resources is influencing across the Horizon Europe programme and is evident across the domain specific aspects of the programme.

This presents a risk of divergence between the communities, researchers and the industrial partners in terms of standards, tools, methods, and approaches. Both the digital and the physical world have encountered significant shocks and the demand for resilience and flexibility is obvious both within industrial ecosystems and the tech developer community.

The positioning of the Cloud-Edge-IoT, and the **development of the federated and autonomous system is evident as a foundational pillar for the realisation of key European aspirations to lead in digita**l. There is an **intercalation between the DIGITAL programme and the Horizon Europe** activities which culminates in the Cloud-to-Edge Large Scale Pilots and the Reference Deployments.

The DIGITAL programme provides common structures, tools and platforms that should be guided and contributed to by foundational building blocks, use cases, and piloting at scale provided for by the cloud-edge-IoT community. The actions of the DIGITAL programme such as the TEFs and Data Spaces act as enablers for further deployment and contextualisation within domain specific and value chain activities across Horizon Europe and leading onto next large scale deployments.

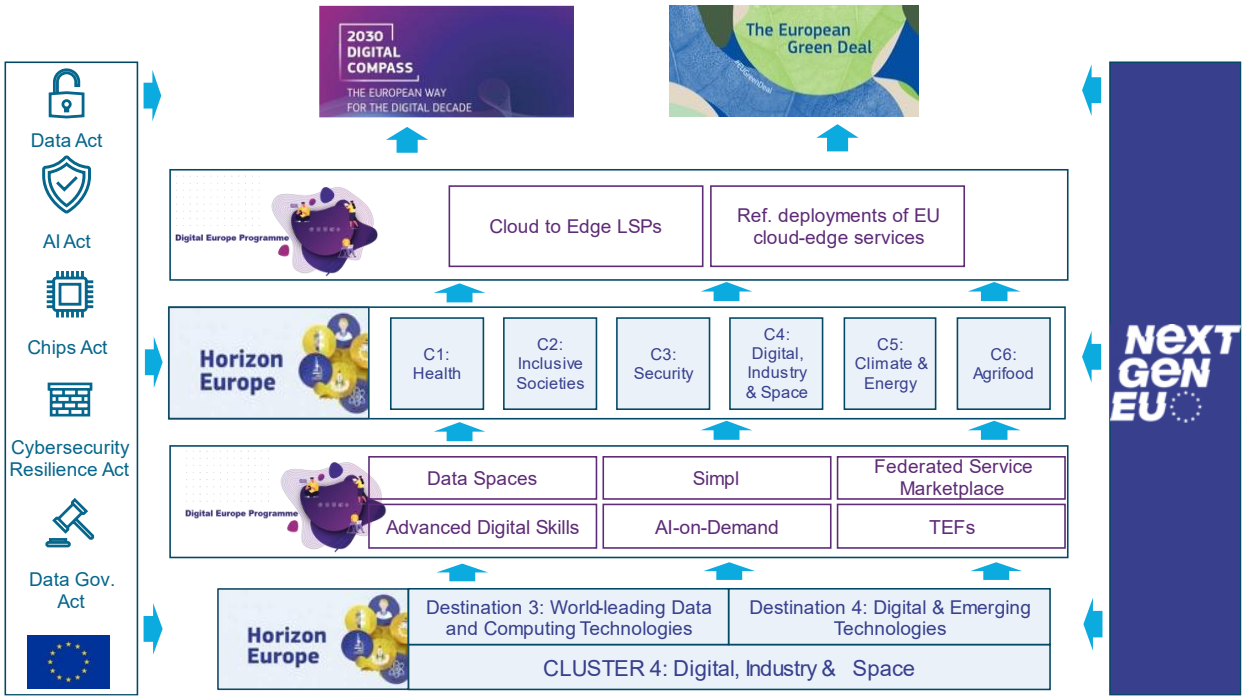


Figure 10. Overview of the European panorama for Cloud-Edge-IoT

Within this decade, the European Union, across Horizon Europe (€15.3 billion), DIGITAL (€7.5 billion), Next Generation EU (€38 billion), multi-county projects and IPCEIs, is putting its weight in the scale of billions of euros of investment behind the creation of a digital infrastructure which promotes ethical use of data, data sovereignty, identity management, resilient and efficient networks, and the security of digital supply chains.

While historic and significant this coordinated investment, **the largest tech companies worldwide, are significantly outspending on their own R&D.** In 2022 alone, Amazon, Alphabet, and Meta spent 69.5, 37.5, 33.6 billion euros respectively. The leading EU corporate, Volkswagen AG, only spent half at 18.9 billion on its R&D in the same year which is not exclusively on digital. In AI alone, the **shift in the balance from public AI research to the private sector as the financial rewards from AI dominance become clearer**. From 2000-2020 there has been a decrease from c.60% to almost 0% in the development of large-scale AI experiments run by

academics driven by the 300,000x increase in compute requirements. [23]

There is an opportunity to take an **integrated vertical approach to leverage the combined heavy weight of the EU funding instruments to make larger and bigger bets on the Cloud-Edge-IoT**. It requires a stronger positioning for the Destination 4 to create building blocks that follows through onto domain-based applications in other Clusters and across the DIGITAL programme, leveraging at a cross-border level the R&D and innovation investments being made by MS under the Next Gen EU.

6.2 Policy considerations that impact the roadmap

As has been noted, there has been a significant increase in efforts to develop a policy framework that can guide and shape the design, development and deployments of technologies that are adjusted to the needs of Europe's citizens and businesses.

Policy intent and target groups

The proposed regulations are different in scope and reach. In general terms, the closer to the citizen, the more restrictive the provisions. These regulations could be considered **to address known problems that have already arisen through market dominance of a few players, seeking to control risks and tackle harms that have already manifested themselves**. Others might be seen to play a **more forward-looking role, seeking to enable innovation** by providing legal certainty and a future-proof framework for operation:

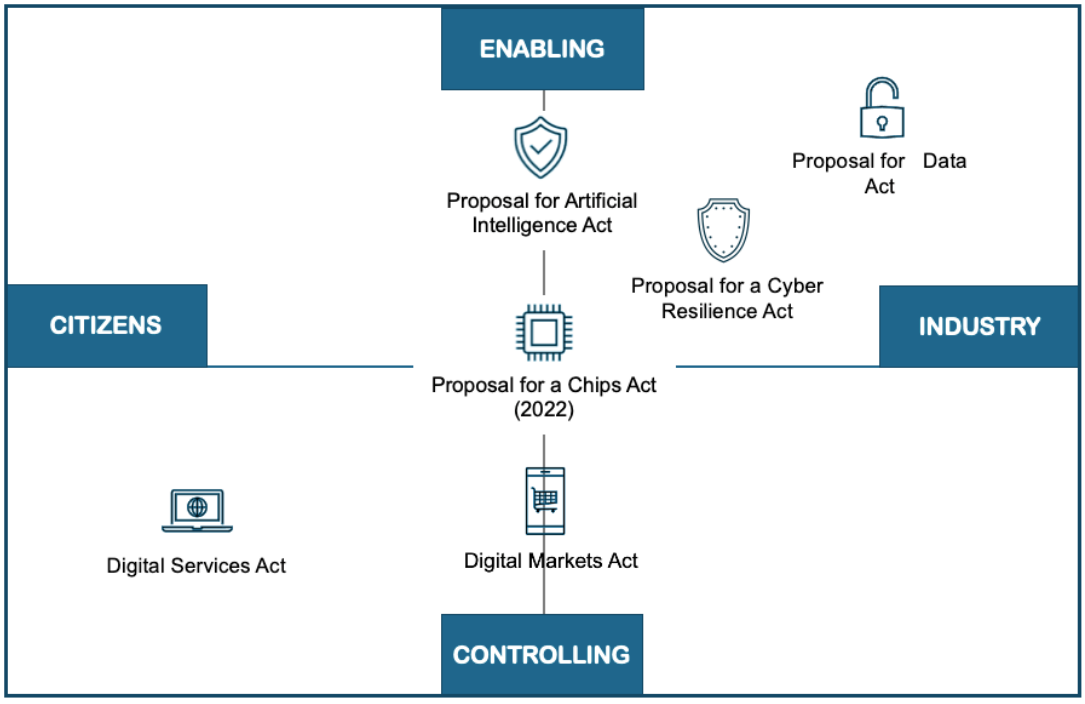


Figure 11. Mapping relevant regulation by focus and characteristics

Varying degrees of relevance

It is also worth noting that the proposed regulations impact on the different NG-IoT building blocks to differing degrees. The following figures provides a high-level indication of where each of the

[23] State of AI 2022

preceding regulations has the greatest relevance:

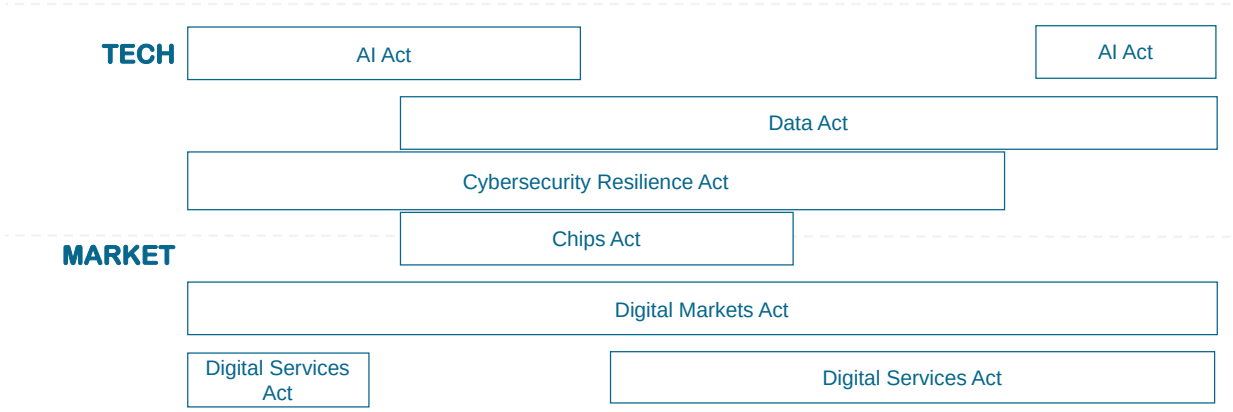


Figure 12. Mapping relevant regulation onto the NG-IoT

Within these, the (proposed) acts that are likely to have most direct impact on multiple fronts on the NG-IoT are the AI Act and the Data Act.

Balancing NG-IoT obligations and opportunities

The **Data Act is one of the regulations that is most likely to impact the Cloud-Edge-IoT Continuum**, requiring several adjustments to the status quo. For instance:

- It is likely to require adjustments to the purchase, leasing or renting agreements to clearly define how data is generated, used and made accessible.
- It intends to protect SMEs by ensuring fair terms of agreement within data sharing contracts through the application of an unfairness test and a model contract to support the evaluation and negotiation of such agreements[24].

For the **operator of cloud and edge platforms, the act creates a significant set of obligations to enable the switching and multi-vendor environment for users through the portability of the assets** and the establishment of the responsibility towards ensuring '*functional equivalence*' when switching to a comparable service. It requires the platform providers to develop the mechanisms to facilitate this and to provide the interfaces and adhere to interoperability standards and the responsibility to ensure the security and integrity of the data.

The regulation defines the roles and responsibilities of operators of data spaces to ensure compliance with the data sharing requirements including the relevant documentation and technical interfaces for automatic and continuous data transition and the minimum requirements for robust smart contracts (such as an emergency stop and rest button) as both are seen to be enablers for the execution of the actions within the regulation.

Consequently, the **NGIoT and CEI stakeholders will be required to consider the design of their systems and architectures to provide the necessary functions** and develop the data

[24] The *sui genesis* claim (i.e. the investment in the creation of a database was significant and should be protected) under the Directive on the Legal Protection of Databases does not apply – cannot be used as a reason for denying access to user-generated data.

interfaces with secure authentication that will be required to put the regulation into action.

Existing data will need to be mapped and sliced based on users for traceability and compliance with requests. It will drive the development of interoperability standards within cloud computing to overcome the current technical barriers to portability, as well smart contracts that facilitate authenticated and controlled sharing between parties.

'Minimum functionality' must be maintained and suitable standards and approaches will be required to define what minimum functionality and switching capacity from a technical point of view. The Commission may drive this through ETSI or similar.

In respect of the proposed AI act, there are several AI practices that are prohibited (eg. AI for real-time biometric identification unless expressly allowed in the Act). high-risk AI systems[25] require establishing, implementing and documenting a risk management system that is able to analyse the risks associated with the AI, both in relation to intended and reasonably foreseeable misuse. There are **specific provisions for training of models with data, requiring that any personal data is only processed to ensure bias is monitored**, and is protected with state of the art security and privacy-preserving measures.

Other important provisions include:

- The obligation to draw up technical documentation before the system is placed on the market.
- Automatic recording of events (´logs´) while the AI system is operating.
- Ensuring sufficient transparency.
- Incorporating human-machine interface tools to enable natural persons to oversee the AI system when it is in use.
- Affixing the CE marking to indicate conformity.

It also provides for voluntary Codes of Conduct that will include requirements in relation to environmental sustainability, accessibility, stakeholder participation in design and development, diversity in development teams etc.

[25] Defined in Art. 6

7 RECOMMENDATIONS AND CALLS TO ACTION

The policy landscape is far from static, with several regulations still requiring the final seals of approval by the Union's legislative bodies. Once approved, certain regulations, such as the AI Act, will still be subject to regular reviews to allow for the rapid evolution of technology.

As things stand, the large-scale pilots present across Horizon Europe and Digital Europe can take some pre-emptive measures to support future compliance. Some could also be used to explore challenges and opportunities within the open calls that invite new stakeholders to continue to innovate and explore new technological applications. With this exploration in mind, the recommendations below provide some initial ideas on measures that could be taken to test both rights and obligations in the practical setting of the CEI large scale-pilots.

7.1 Accessing new resources and capabilities

1. **OPPORTUNITIES TO DEVELOP NEW PRODUCTS & SERVICES INDEPENDENTLY OF CORE PLATFORM PROVIDERS**

   Under the data portability conferred by the proposed Digital Markets Act, business users may offer new services to end users acquired through the core platform services that are considered to be gatekeepers, independently of that platform. This will in theory help business users avoid vendor lock-in and migrate to alternative providers, effectively opening up opportunities for SMEs and others to develop new products and services that are built on the data gathered from the platform, but without the need to continue to use the core platform. [26]

   If they do wish to continue to use the platform, the provider must allow the business user or third-party authorised by them to access "free of charge, with effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data". This is akin to the provisions made in PSD 2[27] that led to innovation in banking services.

2. **CAPACITY TO DEMONSTRATE ADDED-VALUE SERVICES THROUGH STARTUP AND SME ENGAGEMENT**

   The flow of non-personal data is expected to launch a secondary market of data processors who can develop value-added services on top of connected products. In this respect, the open calls could consider encouraging the development of common data spaces within each of the large-scale pilots. There are precedents for this in the opening up of data by the European Space Agency. Any such initiatives should seek to prove evidence of commercially viable solutions while demonstrating the technical opportunity for third-party access and development.

7.2 Built-in compliance

1. **SOLUTIONS AND STANDARDS TO SUPPORT FUNCTIONAL DATA PORTABILITY**

   Any stakeholder classified as a gatekeeper under the proposed Digital Markets Act must ensure that the business user's data is effectively portable. This is further reinforced within the Data Act for cloud and edge platform providers who will be required to define the technical tools and mechanisms for securing portability across services ensuring functional equivalence. Future pilots could therefore explore interoperability standards that

[26] Different conditions apply to personal data, the use of which must be permissioned.

[27] Payment services (PSD 2) - Directive (EU) 2015/2366

might support the portability of digital assets, and the opportunities and challenges that are opened up by the possible integration of multi-provider environments including overcoming challenges where solutions are built on models that cannot be easily ported. New platforms and systems should be able to demonstrate this portability in practice and work across all verticals to provide inputs to common minimum interoperable requirements that can in turn feed into the development of European open standards.

2. COMPLIANT HIGH-RISK AI SYSTEMS

In practice, most of the obligations laid out in the proposed AI act refer to so-called High-Risk AI systems. These include systems[28] which rely on the biometric identification and categorisation of natural personas, as well as systems deployed in the management and operation of critical infrastructure.

Any future CEI pilot must be able to ascertain whether it involves the design and deployment of high-risk AI and take measures to ensure compliance is built in at the earliest stage possible by:

- Developing and implementing risk management systems.
- Ensuring training, validating and testing data sets are subject to appropriate data governance and management practices.
- Drawing up the required technical documentation.
- Establishing appropriate record-keeping measures, including event logs.
- Designing systems that afford the greatest transparency to users, enable human oversight and provide clarity on expected lifetime and maintenance.
- Developing them in a way that ensures accuracy, robustness through technical redundancy or other measures, and addresses cybersecurity measures designed to prevent data poisoning or model flaws.

A Responsible Research and Innovation (RRI) approach to the deployment of intelligence products and services could be considered, bringing the consumer into an active and prosumer role. The aim would be to provide user agency in high-risk AI scenarios. The pilots could provide a controlled environment for this exploration that could start to establish a common European playbook and tools to be used by other AI providers, importers, and distributors.

3. ENABLING TECHNOLOGIES BEHIND COMPLIANCE-BY-DEFAULT

Data spaces and smart contracts which meet the compliance characteristics must been seen as the key enablers and be integrated into the architectures and activities of the pilots that provides the interface security and control for a scaled access to data by users with automated mechanisms that are trialled and adopted within industry to reduce the burden on device manufacturers and support the user acceptance.

4. MONITORING AND MEASUREMENT OF DATA ACT

The provision of a longitudinal study which monitors the impact of the Data Act within the CEI community, markets and within society will provide the evidence for its continued implementation, providing a proactive approach to compliance on both sides. This will identify best practice, sharing of common tools and solutions and provide foreword intelligence on future barriers and challenges for where technical solutions can reduce friction and ensure a dynamic and competitive Single Market.

[28] The full list of High-risk AI systems in article 6(2) of the AI Act can be found in Annex.

7.3 Supporting a future-proof CEI

1. **FULL VERTICAL INTEGRATION AND LARGE SCALE INVESTMENTS**

   The CEI is the foundation of Europe's digital future and requires significant investment in the coordinated and collaborative development. A focus of the Cloud-Edge-IoT is to provide the building blocks for reliability, trust and efficiency to be developed and advanced within domain contexts with a clear journey and roadmap towards large scale deployment with an emphasis on market entry or market creation.

   The cross-SRIA analysis has demonstrated the common base of the Cloud-Edge-IoT for wholescale digitalisation of European industries and as such the definition of any Large-Scale Pilots should be industry led in setting market vision and ambition with enough scale and scope to provide a credible challenge to the current market status quo. There should be a combination across HE clusters, DIGITAL and other investment sources like the EIB to reach these goals and provided as tailored constructions led by both the Digital Decade and Green Deal.

2. **INVESTING IN MARKET READINESS**

   The success of the European federated vision will depend on the value derived by businesses and the stimulation of private investment in new IT and OT resources including the upskilling and reskilling of operators and technicians. Market studies and collaborative foresight and business case development along value chains is an ongoing task and necessary route to impact which tracks along tech development roadmaps and provides a reactive and adaptive R&I community.

   Another key pillar of Market Readiness is the topic of digital skills. Direct links between the CEI communities and the Advanced Digital Skills component of the Digital Programme should be fostered and a direct link to the training and vocational education bodies to address future skills demands and strategy roadmaps which accompany each key tech priority area.

3. **TEMPLATES & TOOLS FOR ADVANCED CE MARKING AND CERTIFICATION**

   The development of self-assessment criteria for risk of AI products will require specific support. Technical tools deployed in pilot setting might be able to facilitate compliance-by-default. and coordinate contributions towards the development of codes of conduct mentioned above. Related to this, is the expected requirement that all developed solutions are CE marked. This in turn could provide an opportunity to collaboratively design a process with the pilot stakeholders and experienced actors from the market surveillance sphere.

4. **A COLLABORATIVE AND ACTIVE REGULATOR**

   There is a role for non-traditional actors in the activities of the pilots, specifically involving regulatory bodies and other public bodies who should be considered key stakeholders and direct participants in the CEI community. The development of an AI Act compliance database and platform within the DIGITAL programme will facilitate the relationship between the Market Surveillance Authorities as they upskill to this new role. In the meantime, however, the engagement of National Sandboxes should be a priority of the Large Scale Pilots and support the development of case studies and leading solutions within high-risk domains of Health, Public Services, Smart Communities and eGovernment.

8 ANNEX

Table 8 Comparison in scope (Article 1) between Initial proposal and the March 13th Parliamentary Approved Proposal

Def Nr	COM (2022) 68 FINAL Feb 22	P9_TA(2023)0069 Mar 23	DEFINITION (**bold** wording reflects incorporation to the Parliamentary Approved Proposal)
1	Data	Data	Means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording; **Content, or data obtained, generated or collected by the connected product or transmitted to it on behalf of others for the purpose of storage or processing, shall not be covered by this Regulation**.
1a		Personal Data	**Means personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679; "Means any information relating to an identified or identifiable natural person".**
1b		Non-personal Data	**Data other than personal data**
1c		Consent	**Means consent as defined in Article 4, point (11), of Regulation (EU) 2016/679 "Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".**
1d		Data Subject	**Means data subject as defined in Article 4, point (1), of Regulation (EU) 2016/679 "An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."**
1e		Data User	**Means a natural or legal person who has lawful access to certain personal or non-personal data and has a right to use that data for commercial or non-commercial purposes.**
2	Product	**Connected**	An item, that obtains, generates or collects, **accessible** data concerning its use or environment,

		Products	and that is able to communicate data via **an electronic communications service, a physical, connection or on-device access** and whose primary function is not the storing, **processing or transmission of data on behalf of others.**
3	Related service	Related Services	Means a digital service, including software , but excluding electronic communication services which is inter-connected with a product in such a way that its absence would prevent the product from performing one or more of its functions, **and which involves accessing data from the connected product by the provider or the service.**
4	Virtual assistants	Virtual Assistants	Means software that can process demands, tasks or questions including those based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access to other services or control **the functions of products**.
4a		**Consumers**	**Means any natural person who, is acting for purposes which are outside that person's trade, business, craft or profession**
5	User	Users	Means a natural or legal person that owns **a connected product or receives a related service or to whom the owner of a connected product has transferred, on the basis of a rental or leasing agreement, temporary rights to use a connected** product or **receive related** services **and, where the connected product or related service involves the processing of personal data, the data subject.**
6	Data holder	Data Holder	Means a legal or natural person, who has **accessed data from the connected product or has generated data during the provision of a related service and who has the contractually agreed right to use such data, and the obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law to make** available certain data **to the user or a data recipient**
7	Data recipient	Data Recipient	Means a legal or natural person other than the user of a connected product or related service, to whom a data holder makes **available data accessed from a connected product or generated during the provision of a related service** following an explicit request by the user or in accordance with a legal obligation under Union law or national legislation implementing Union Law.
8	Enterprise	Enterprise (No changes made)	Means a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person's trade, business, craft or

			profession.
9	Public sector body	Public Sector Body (No changes made)	Means national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies
10	Public emergency	Public Emergency	Means an exceptional situation, **limited in time such as public health emergencies, emergencies resulting from natural disasters, as well as human- induced major disasters, including major cybersecurity incidents,** negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, **financial stability**, or the substantial **and immediate** degradation of economic assets in the Union or the relevant Member State(s) **and which is determined and officially declared according to the relevant procedures under Union or national law**
10a		**Official Statistics**	**Means 'European statistics' within the meaning of Regulation (EC) No 223/20091; "Usually based on national data produced and disseminated by the national statistical authorities of all Member States, they may also be produced from non-published national contributions, subsets of national contributions, specifically designed European statistical surveys or harmonised concepts or methods".**
11	Processing	Processing	Means any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
12	Data processing service	Data Processing Service	Means a digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature;
13	Service type	Service Type	Means a set of data processing services that share the same primary objective and basic data processing service model
14	Functional equivalence	Functional Equivalence	means the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input

			action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract
15	Open interoperability specifications	Open Standard	**Mean** technical specifications, which are performance oriented towards achieving interoperability between data processing services **and which are adopted through an inclusive, collaborative, consensus-based and transparent process from which materially affected and interested parties cannot be excluded.**
16	Smart contract		*(Deleted from Scope Section)*
17	Electronic ledger		*(Deleted from Scope Section)*
18	Common specifications	Common Specifications (No changes made)	Means a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation;
19	Interoperability	Interoperability	Means the ability of two or more **data-based serviced, including** data spaces or communication networks, systems, products, applications or components to **process**, exchange and use data in order to perform their functions **in an accurate, effective and consistent manner**
19a		**Portability**	**Means the ability of a customer to move imported or directly generated data that can be clearly assigned to the customer between their own system and cloud services, and between cloud services of different cloud service providers**
20	Harmonised standard	Harmonised Standard	Means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation
20a		**Common European data spaces**	**Means purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, development of new products and services, scientific research or civil society initiatives;**
20b		**Metadata**	**Means a structured description of the contents of the use of data facilitating the discovery or use of that data**
20c		**Data**	**Means data intermediation service as referred to in Article 2, point (8), of Regulation (EU)**

		intermediation service	**2022/868 " Means a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, excluding at least the following**
20d		**Data altruism**	**"Means the voluntary sharing of data as defined in Article 2(16)of Regulation (EU) 2022/868 "means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest”"**
20e		**Trade Secret**	**Means information which meets all the requirements of Article 2, point (1) of Directive (EU) 2016/943; " ‘trade secret’ means information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."**
20f		**Trade Secret Holder**	**Should be understood as per Article 2, point (2) of Directive (EU) 2016/943. ‘trade secret holder’ means any natural or legal person lawfully controlling a trade secret;**