Grant Agreement N°: 956671

Topic: ICT-56-2020

The European IoT Hub

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

D2.5: NGIoT Roadmap and Policy Recommendations

Revision: v.1.1

Work package	WP 2
Task	Task 2.3
Due date	30/03/2022
Submission date	03/05/2022
Revision date	05/09/2022
Deliverable lead	BluSpecs
Authors	Tanya Suárez (BluSpecs), Brendan Rowan (BluSpecs)
Version	1.1
Dissemination level	PUBLIC

TABLE OF CONTENTS

LIST OF FIGURES

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
CSA	Coordination and Support Action
CTF	Communication Task Force
DEI	Digitising European Industry
DEP	Digital Europe
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 ecosystem is evolving, and how the policy framework, which is currently under development, is likely to impact this evolution in the future. The aim is to provide tailored 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 the start of 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 currently under development. As such, it hopes to set the ground for the input that will be gathered from experts and Cloud-Edge communities over the next few months. An updated version will be published in March 2023, with updated content on the strategic research agendas and the regulatory framework.

Finally, it is worth noting that this is a first report. A second report is due in Q1 of 2023. This will delve deeper into the policy implications will become clearer as the proposed regulations are amended, approved, and explored by the NG-IoT community.

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 paradigm, 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 too the dynamic policy measures that are currently under development.

NGIOT: Roadmap for IoT Research, Innovation and Deployment in Europe 2021-2027[1]

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.

Horizon CLOUD: Cloud Computing in Europe[2]

Horizon CLOUD applies a supply and demand approach to enabling digital transformation through cloud adoption. It offers recommendations, structured around four key pillars:

- Data Aware Organisations
- Data-driven Innovation
- Strengthening the EU Market, and
- Foundational Elements.

This complements an earlier comprehensive strategy report which analyses and defines the major challenges facing cloud computing providers and adopters. It addresses in detail the demand domains of energy, transport, agriculture health and manufacturing with a specific focus on SMEs and the supply side.[3]

EU-IoT produced mapping and analysis

In addition to the above external reports, the EU-IoT consortium has already provided significant mapping and scoping reports and activities contained within the following documents:[4]

- 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.

---

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

[2] Cloud Computing in Europe: Landscape Analysis, Adoption Challenges and Future Research and Innovation Opportunities, White Paper, Version 1.6, (2022), Dietrich M., Facca, F. *et al,* H-CLOUD CSA Consortium

[3] Strategy analysis report and Cloud Computing, (2021), Dietrich M. *et al*, H-CLOUD CSA Consortium

[4] Publicly available through the NGIoT Portal: www.ngiot.eu/deliverables

- 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.
- D3.5 Mapping of Knowledge Areas to Standardisation V1.0
- Maps the principal technologies and knowledge areas from 3 strategic research and innovation agendas against Horizon Europe clusters and SDOs.
- D3.7 Recommendations on research priorities and innovation strategies to standardization v1.0
- Presents the mapping of the key areas of standardisation and relevant bodies for the research and innovation activities across the ICT56 RIAs (NGIoT Initiative).

2 THE NEXT GENERATION IOT

2.1 Overview

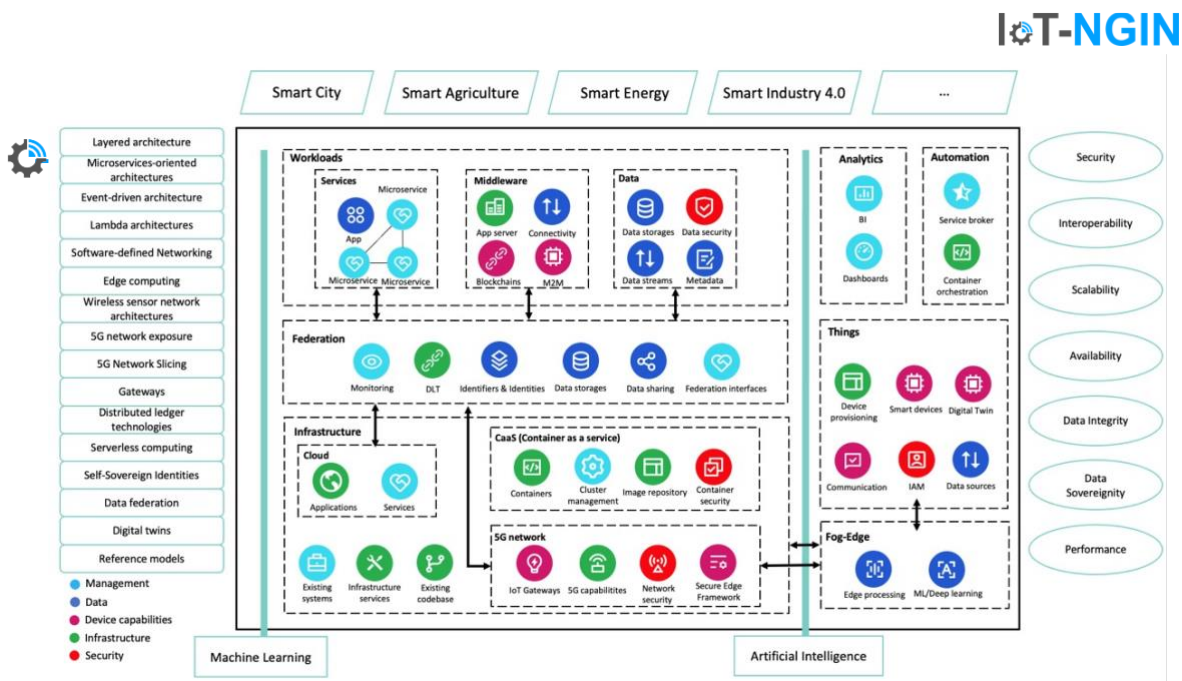
The exact definition of the IoT has been attempted by various bodies, from the IEEE definition based on a description of the constituent elements, to the ITU's definition focusing on what is achieves. The definition used in the NGIoT Roadmap encompasses both, describing the IoT as "*a system of systems that have (at least) the following properties: Sensing and actuation, Connectivity, Intelligence, Heterogeneity, Dynamicity, Scalability, Security*".[1]

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.[5]



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

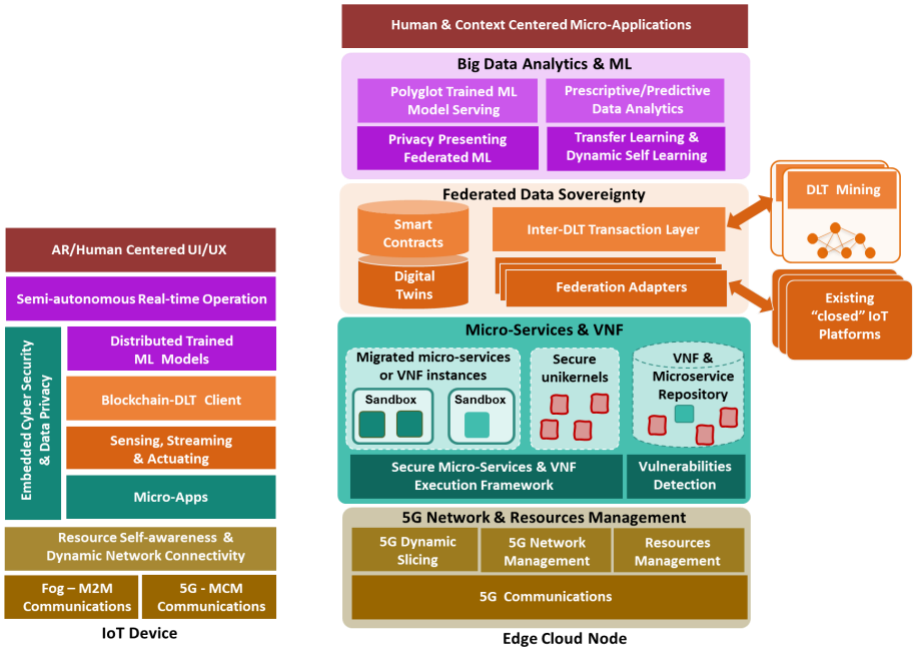


Figure 1. Overview of the IoT NGIN meta-architecture (above) and high-level (below) demonstrating the integration of multiple technologies and microservices with novel and secure interfaces

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).

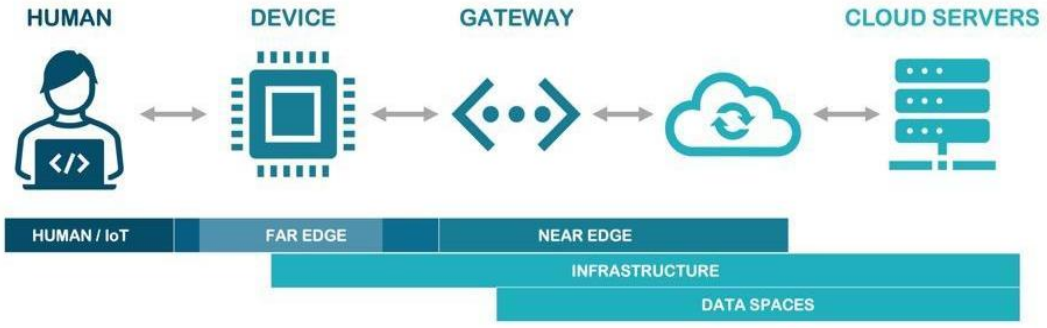


Figure 2. The IoT continuum. From human to cloud and back again with key interfaces.

Within these five key contexts, which bracket 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).
- Standards and policies: delving into common approaches, standards, and policies.
- Skills: analysing the current and future demands resulting from all the above

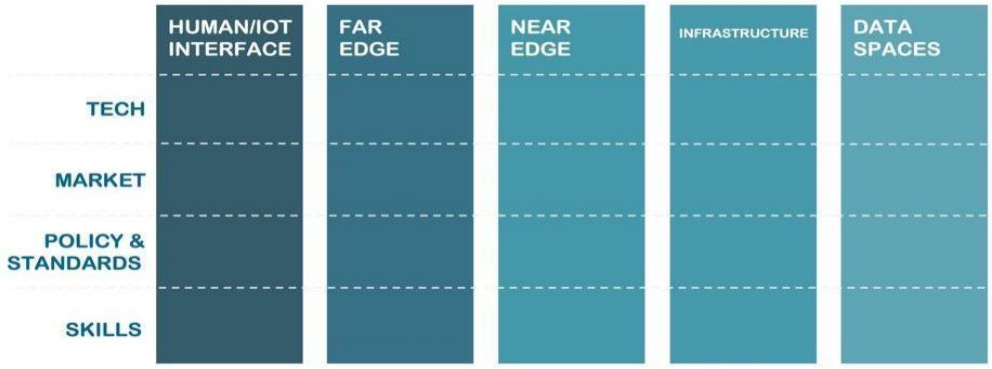


Figure 3. Guiding framework of the EU-IoT approach

3 STRATEGIC TOPICS AND THEMES RELATED TO THE NGIOT

3.1 Summary of relevant Strategic Research and Innovation Agendas

There are several industry associations and research partnerships that develop Strategic Research and Innovation Agendas (SRIAs) that relate to the NG IoT. These agendas map out the trends and priorities, providing guidance for their respective members, communities, as well as policy-makers, allowing for alignment of investments and actions.

Some analysis of this content had already been addressed in the Deliverable 3.5 *Mapping of Knowledge Areas to Standardisation*[6], which provides the individual mapping of the technology and knowledge areas towards the Horizon Europe Clusters.

This analysis, however, focuses more specifically on the identification of common themes and trends across the relevant communities for the NGIoT. The SRIAs that have been included in the analysis include the following:

- Strategic Research, Innovation and Deployment Agenda, AI, Data & Robotics Partnership, September 2020 (BDVA/DAIRO, CLAIRE, ELLIS, EurAI, EURobotics).
- European industrial technology roadmap for the next generation cloud-edge offering, May 2021, European Alliance for Industrial Data, Edge and Cloud.
- ECS: Strategic Research and Innovation Agenda 2021 (Aeneas, Artemis-IA, EPoSS).
- Made In Europe: The manufacturing partnership in Horizon Europe Strategic Research and Innovation Agenda, September 2021, (EFFRA).

The latest SRIA from AIOTI is in the final stages of preparation and will be later integrated into the second version of this document.[7] This second version will revise the later versions of such documents produced across all associations and make a comparison to the current analysis to detect changes in directions, emerging themes, and relative importance.

3.2 Identification of overarching themes

Defining and categorising topics

There are 146 distinct topics present in the SRIAs and associated documents, which can be broadly classified as follows:

- Priority areas: considered to be topics of strategic importance, encompassing multiple technologies and applications. E.g., Constraint-based planning and decision making in complex natural environments.
- Applications: specific implementations of technologies either within a given context or addressing a defined goal. E.g., Data streaming in constraint environments.
- Technologies: a variety of different technical, electronic or physical systems, assets, devices or algorithms. E.g., Self-configuring and adaptive sensor nodes.

Common themes

The topics above were clustered with related topics under a set of themes which cover multiple

[6] D3.5 Mapping of Knowledge Areas to Standardisation Version 1; EU-IoT Consortium

[7] A high-level review of the AIOTI key technology areas to be developed within this document can be found in the annex to Deliverable D3.5 and has been included here.

topics as shown in the chart below.

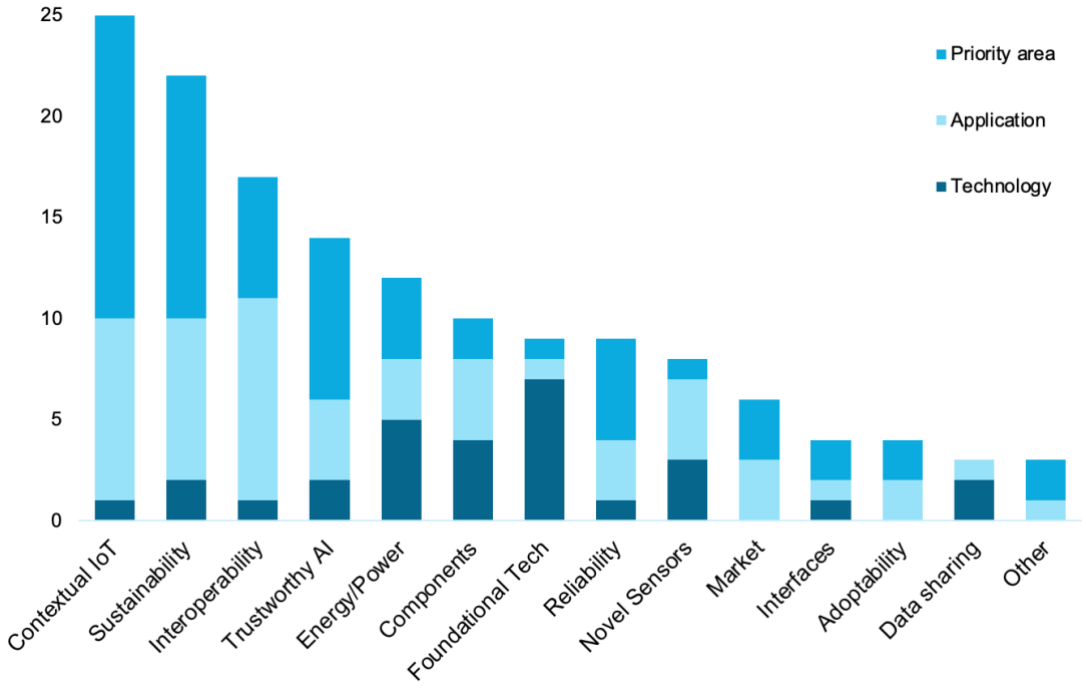


Figure 4. Key themes present across SRIAs by number of associated topics mentioned

Contextual IoT is the most common theme. It covers efforts to address the application of IoT within constrained environments for relevant and autonomous/semi-autonomous decision-making. This includes:

- Operation within domain-specific models,
- Adaptation to changes within the environment,
- Planning for and dealing with uncertainty and complex natural environments and
- Integration of multi-agent and human inputs.

BDVA/DAIRO are particularly active here, addressing the role of AI across these areas.

Sustainability is a clear goal within the analysis and is a driver of technology development. It is particularly relevant for ECS, followed by the Industrial Cloud-Edge-IoT Alliance and EFFRA. Sustainability addresses the need to develop a technology stack that is itself sustainable by design and planning for extended lifetime operation and a circular economy approach through mechanisms for achieving reduced obsolescence, component recyclability, application of the technology to decarbonise and reduce energy consumption across industries, and the integration of legacy systems through virtualisation and other means.

Interoperability, while implicit in other themes such as Contextual IoT, Sustainability and Data Sharing, is third in overall importance, including modular design of software and platforms within an SoS (system of systems) context and constrained environments. It is seen as a key lever for the scalability of the developed technologies and management of performance of the system as a whole within platforms. It requires the establishment of standards and approaches to engineering that can facilitate adoption across the whole value chain.

A more specific theme is related to the development of AI that is trusted by the humans both deploying it and those who are affected by it. This is addressed by the following topics:

- The preservation of security and that of the models and algorithms

- Preservation of privacy throughout entire data processing cycle
- Zero-trust identification management
- *Explainability* of the recommendations and/or decisions made.

Elements of trust are also present within Contextual IoT[8] and reliability, the latter addressing the robustness of the system as a whole, rather than the discrete AI component of the solution.

There is also a clear demand for low power consumption within sensors and devices, even attempting to approach zero energy systems (powered by ambient energy). The goals are to balance power and performance; reducing the energy footprint of the systems, developing climate neutral edge nodes, active and advanced cooling systems and achieving efficient cloud and high-performance computing. This particularly a priority for the component and cloud communities.

The development of next-generation components is a key aim of all the SRIAs. Components refer more to software and middleware to support the integration of the devices to the cloud and the rolling out of novel hardware accelerators with a flexible system of cloud and edge computing. As a separate but related sub-theme, novel sensors are required that are wearable, self-configuring and contributing to heterogenic data sets, with a new class of chemical and bio-based sensors which can accurately identify and quantify small-molecules on a picomolar scale.

There is a need for foundational technology development which covers advanced radio frequencies and photonics (infrastructure), silicon technologies and wafer fabrication (devices), quantum computing (HPC) and satellite IoT as both communications and acting as an edge-node.

Other topics of note include specific business case driven applications, methods for reducing the barriers to adoption and the virtualisation of legacy systems and integration of existing embedded systems within the NGIoT systems.

THEME	AI, Data, Robotics	AIOTI	ECS	Cloud Alliance	EFFRA
CONTEXTUAL IOT	84%		4%		12%
SUSTAINABILITY	5%		55%	23%	18%
INTEROPERABILITY	6%	6%	47%	6%	35%
TRUSTWORTHY AI	50%	7%	21%	14%	7%
ENERGY/POWER	8%	8%	50%	33%	
COMPONENTS		20%	40%	10%	30%
FOUNDATIONAL TECH		11%	44%	33%	11%
RELIABILITY	11%	33%	33%	11%	11%
NOVEL SENSORS	63%		13%		25%
MARKET				50%	50%
INTERFACES	75%	25%			
ADOPTABILITY	50%				50%
DATA SHARING			33%		67%
OTHER			67%		33%

Figure 5. Relative distribution of themes by source using non-normalised data

[8] This overlap of topics across these two themes may be related to the difference in terminology and priorities between the AI, Data and Robotics Partnership and the ECS cooperation.

Notably absent from the above themes are those topics related to orchestration and container-based solutions for migrating applications to the edge with context awareness, flexible networks for a programmable, multi-purpose general infrastructure through network virtualisation, resilient microservices architecture beyond REST and AI/ML-as-a-Service for a prosumer approach to edge-AI. These topics are dealt with in detail within the NetWorld2020 SRIA[9] led by the previous 5G-PPP and are currently being addressed by the ICT 56 RIAs which form the NGIoT Initiative and are present in the road mapping conducted in D2.1 and D2.2 EU-IoT deliverables.

3.3 Contextualisation within the NGIOT framework

Mapping the topics within the EU-IoT framework, some trends and gaps can be observed within the whole picture of the NGIoT. As would be expected from Strategic Research and Innovation Agendas, there is a particular emphasis on the TECH layer, doubling the number within the Market layer with a much lower level in Standards. As already identified in a previous report[10] and the work with the EU-IoT Expert Group, the element of Skills is rarely addressed and presents again a significant weakness in the development of the NGIoT with a single reference across the nearly 150 topics.

Examples of clusters of topics within the most popular layers include:

- TECH: human interrogation for decision making, seamless identification, multimodal interfaces, and the perception of non-verbal cues, high-performance ultra-low power 3D integration, system energy conservation in software and hardware design and integration.
- MARKET: Scalable attestation of IoT safety, extending the lifetime of products and services, modular multifunctional systems for production, risk management within cascading effect.
- STANDARDS: Zero trust identity management, low carbon data storage protocols, sustainability KPIs within cloud, edge cybersecurity.

All	HUMAN INTERFACE	FAR EDGE	NEAR EDGE	INFRA STRUCTURE	DATA SPACES	ALL	OTHER	
TECH	18	31	6	7	2	12	3	**79**
MARKET	5	7		3	6	15	4	40
STANDARDS	2	9	2	2	7	2	2	26
SKILLS						1		1

Figure 6. Distribution of all topics within the relevant SRIAs mapped against the EU IoT framework

From across the different continuum contexts, the Far Edge accounts for 32% of all topics, followed by All (21%), which are topics that touch on all contexts. Human Interfaces follows closely with 17% with around 10% for Data Spaces (i.e. cloud computing and data sharing). Of note is the lower focus on Infrastructure and Near Edge research and innovation topics at 8% and 5,5% respectively while uncategorised topics (Other) were diverse, ranging from flexible substrate electronics to waste recovery technologies. These amount to 6% of topics found within the SRIAs.

When reviewing the Priority Areas, there appears to be a lack of defined interest in the Near Edge; it is underrepresented within this mapping. While the Far Edge was assigned for topics that were on-device, it was not fully evident when a topic related to edge nodes and gateways and thus broad topics (considered ALL) we found to be covering relevant areas for the Near Edge.

[9] Smart Networks in the context of NGI, September 2020, European Technology Platform NetWorld2020

It would be reasonable to assume that the analysis of applications would reveal a greater population of the Market layer. It appears, though that the applications still require further development of the groups of technologies to enable the different use cases, either driving greater integration of different groups of technologies or tailoring to a specific business context. The applications identified are mostly related to the whole NGIoT continuum or are focused on the Far Edge, following the trend seen for the topics overall.

Priority Areas	HUMAN INTERFACE	FAR EDGE	NEAR EDGE	INFRA STRUCTURE	DATA SPACES	ALL	OTHER	
TECH	9	14		3		2		28
MARKET	3	2		2	4	8		19
STANDARDS	1	4		1	6	2	1	15
SKILLS						1		1

Applications	HUMAN INTERFACE	FAR EDGE	NEAR EDGE	INFRA STRUCTURE	DATA SPACES	ALL	OTHER	
TECH	6	8	3		1	8	1	27
MARKET	1	4			1	6	4	16
STANDARDS	1	5	2	1	1		1	11

Technology	HUMAN INTERFACE	FAR EDGE	NEAR EDGE	INFRA STRUCTURE	DATA SPACES	ALL	OTHER	
TECH	3	9	3	4	1	2	2	24
MARKET	1	1		1	1	1		5

Figure 7. Distribution of all topics within the EU-IoT Framework by type

The shift towards the Far Edge has an emphasis on the development of new components and the creation of a network of intelligent devices. This technology push can be evidence of the expectation that the next-generation of Cloud-Edge-IoT presents an interesting new market. A deeper look into the content of the SRIAs, however, reveals an interest in the orchestration of technologies that will underpin a federated cloud and data spaces, which will create a stronger role for the Near Edge in future use cases and complex systems on the edge. There is also a recognised need to focus on the market demand for the different technologies across the key that are most likely to benefit from the NG-IoT.

Community interests

As could be expected, the analysis of the SRIAs reveal that different communities have varying degrees of interest in the seven themes that make up the Cloud-Edge-IoT continuum:

- The DAIRO Partnership is more focused on the Human Interface and Far Edge as opposed to the Data Spaces and Near Edge.
- The ECS Alliance has a component and engineering focus within the Far Edge and across All themes.
- The work initiated by the AIOTI is currently addressing topics fairly evenly, although greater interest in certain areas may emerge as work progresses.

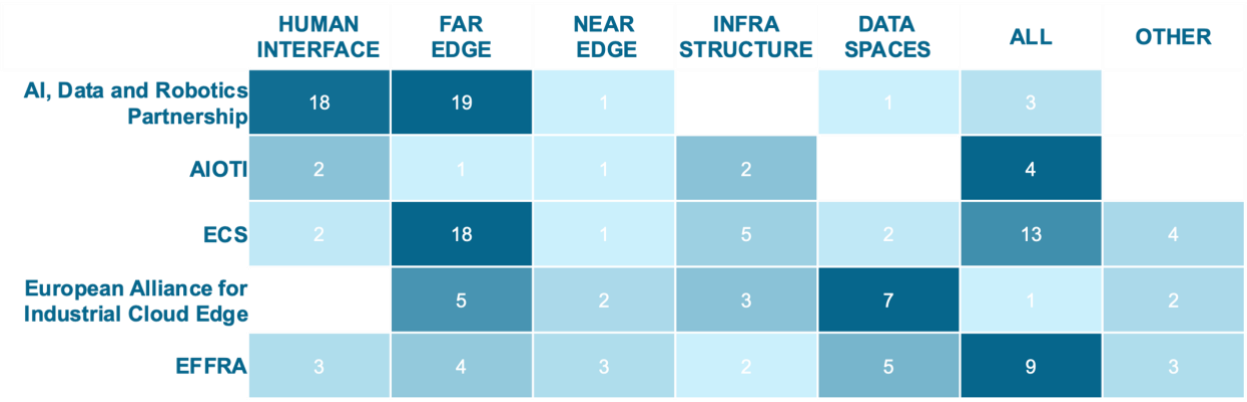


Figure 8. Relative distribution of all topics within individual SRIAs using non-normalised data

4 POLICY ANALYSIS

4.1 A new age for Digital Policy development

From a policy perspective, the past decade has been one in which European political leaders have navigated a myriad of societal and economic challenges, demanding measures that support the emergence of a more resilient and competitive economy and prepare Europe to deal with a less stable global political environment.

The convergence of health, climate, energy and territorial emergencies has required a branch and root transformation of how European businesses and citizens operate and adjust to the digital and green transitions. Ensuring Europe's digital "sovereignty" has become a fundamental part of ensuring its future competitiveness, even underpinning social freedoms.

Throughout this period, the pace of technological development has accelerated and policy-making now, more than ever, must be forward-looking, taking into account how data and technology usage will evolve in the near and more distant future. 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]

4.2 Driving recovery and resilience through a Single Digital Market

Across Europe, policy-makers 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.

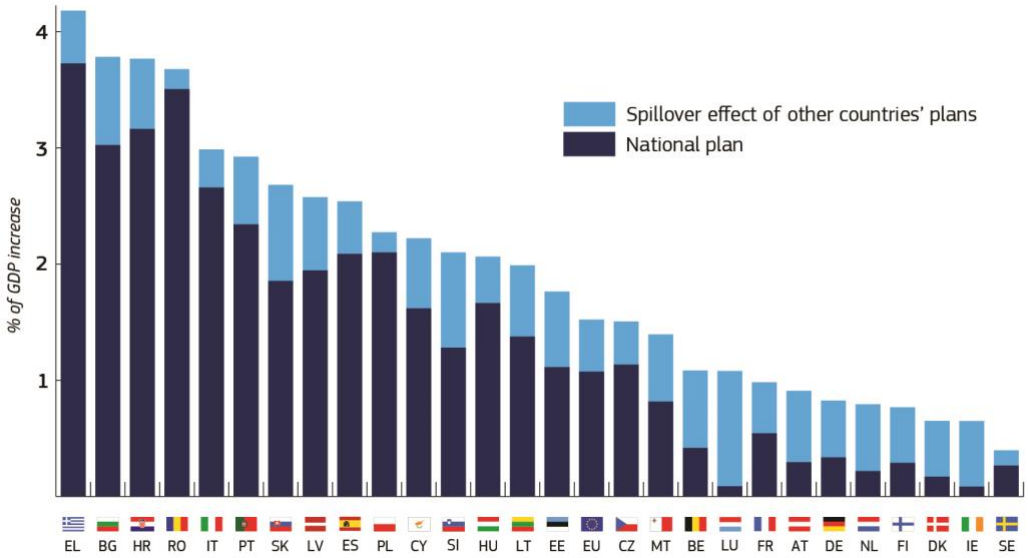


Figure 9. Quantifying Spillovers of Next Generation EU Investment, Discussion Paper July 2021.European Commission.

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

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 increased the importance of reviewing the 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 11, above).

4.3 Overview of main regulations to guide the NG-IoT

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[14] framework that can protect rights, and provide guidance and legal certainty to all stakeholders. From this perspective, the most relevant regulations set to impact the NG-IoT include:

- Proposal for Data Act {SEC (2022) 81 final}
- Proposal for Digital Markets Act {SEC(2020) 437 final}
- Proposal for Digital Services Act {SEC(2020) 432 final}
- Proposal for Artificial Intelligence Act {SEC(2021) 167 final}
- Proposal for a Chips Act (2022) (pending review)

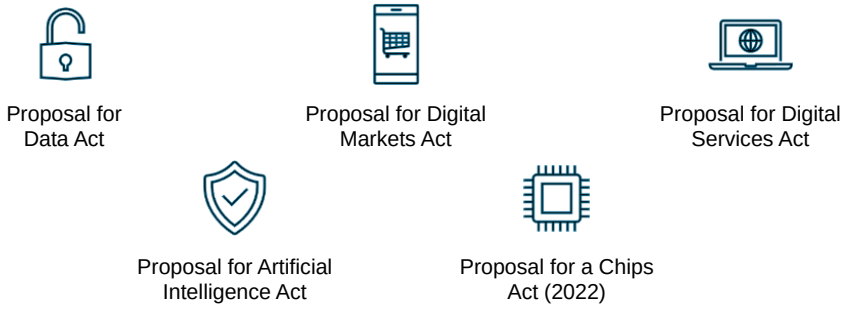


Figure 10. Main regulations that are likely to have a direct impact on the NG-IoT

Each of these confers a distinct set of rights and obligation on different stakeholders in the digital ecosystem, seeking to clarify what can and cannot be done with data in a range of settings. The paragraphs that follow offer a brief description of the proposals as they stand.

4.3.1 Data Act

The proposed Data Act relates to the sharing non-personal data that is generated through the use of connected product or related service by a user from the data holder to the user or a

[12] In current prices.

[13] Across 22 recovery and resilience plans approved to date.

[14] 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.

designated third-party data processor authorised by the user. The data covered within the proposed regulation includes:

- Data in the form and format that is generated by the product.
- Data from related services that are bundled, including that not provided by the manufacturer but a third-party.
- Data arising from the use Virtual Assistants.

Description

The proposed regulation aims to establish a legislative mechanism for ensuring the fairness and access to data by the persons (legal or natural) who generate it through their use of a purchased device or physical item that has connectivity, or associated services. It also explicitly provides for access to essential data by governmental bodies, in cases of exceptional need.

Ultimately, it aims to release access to data to encourage innovation, enable portability across data service providers (e.g., between cloud and edge platforms), and help public bodies access data to respond to crises and societal challenges.

Under the proposed legislation, upon request by the user or consumer, the data holder (device manufacturer, lessor or other) is required to provide access in a useable, continuous and real-time format for the execution of a specific purpose.

This will require data holders (device manufacturers and service providers) to design their products and services in such a way that individual user data can be isolated, treated to remove any personal data (when required) and made accessible for the user or a designated third-party. Data holders are able to charge reasonably for these services to cover the investment made, but the data must be provided at cost to SMEs; in either case, a break down of how this compensation was calculated must also be provided.

The regulation addresses four main areas, summarised in the table following:

Context	Provision
B2B and B2C data sharing and access	• Providing timely and continuous access to the data that is easily, securely and where possible, directly accessed by the user or their authorised third-party at the same standard to which the data holder has access.
Provision of data to public bodies for an *exceptional need*	• Provided free-of-charge when requested as part of a response to a public emergency. • Provided at cost plus reasonable margin when requested to prevent or recover from a public emergency or to overcome a barrier in completing a task in the public interest.
Portability of digital assets from cloud and edge platforms (data processing services)	• Ensuring that platform customers can switch between providers and on-premises servers within 30 days with continuity of service and provision of functions and assist the switching process to completion. • Obliging data processing services to port all data assets which includes data, applications, virtualised machines, etc. • Provide a detailed report and alternative solutions where portability is not technically unfeasible.
Interoperability mechanisms and	• Definition of obligations for the operators of data spaces with

standards	regards to data record and access. • Definition of the essential requirements for smart contract (and their operators) which facilitate the management of the data sharing.
B2B and B2C data sharing and access	• Provide the Commission with the capacity to request and enforce interoperability standards for data spaces, cloud interoperability and smart contract interoperability for the definition of compliance with the requirements and obligations.

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), public bodies.

Main exclusions

- Data inferred or derived from usage of the product or service.
- Data from the use of mobile phones and tablets.
- Personal data; must be requested through a data controller or subject as under GDPR.
- Gatekeepers who are designated under the Digital Markets Act do not have the rights to access or process the data within this regulation.
- Request for data by public bodies as part of activities related to criminal offences, customs and taxation administration, and where the data can already be obtained on the market.
- Disclosure of trade secrets; except where necessary for the execution with agreements in place to ensure confidentiality.
- Proprietary data and IPR belonging to the data holder.
- Sector-specific needs within data sharing.

There are specific exclusions for SMEs, who are not required to comply with design obligations except where it is a sub-contractor for the design and manufacture of a product; exempt from the obligations related to the sharing of data generated by the use of their products or related services; not required to comply with data requests from public authorities.

4.3.2 Proposal for a Digital Markets Act

Applies to core platform services provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and of other law otherwise applicable to the provision of service.

Description

The proposed regulation lays down harmonised rules ensuring contestable and fair markets in the digital sector across the Union where gatekeepers are present. It applies to core platform services provided or offered by gatekeepers to business users. Core platform services means any of the following:

- online intermediation services;
- online search engines;

- online social networking services;
- video-sharing platform services;
- number-independent interpersonal communication services
- operating systems;
- cloud computing services;
- advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the above.

At the heart of the regulation is the figure of the 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.

Stakeholders

Gatekeepers, competitors, business users, consumers, regulatory authorities.

Main exclusions

Electronic communications networks and electronic communications services. [15]

4.3.3 Proposal for a Digital Services Act

The Regulation aims to contribute to the proper functioning of the internal market for intermediary services and set out uniform rules for a safe, predictable and trusted online environment, to protect fundamental human rights.

Scope

It applies to intermediary services provided to recipients of the service who are established or resident in the Union, irrespective of the place of establishment of the service providers.

Tailored asymmetric obligations

	Intermediary services	Hosting services	Online platforms	Very large platforms
Transparency reporting	●	●	●	●
Requirements on terms of service due account of fundamental rights	●	●	●	●
Cooperation with national authorities following orders	●	●	●	●
Points of contact and, where necessary, legal representative	●	●	●	●
Notice and action and obligation to provide information to users		●	●	●
Reporting criminal offences		●	●	●

[15] As defined in point (1) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council. as defined in point (4) of Article 2 of Directive (EU) 2018/1972 other than those related to interpersonal communication services as defined in point (4)(b) of Article 2 of that Directive

Complaint and redress mechanism and out of court dispute settlement			●	●
Trusted flaggers			●	●
Measures against abusive notices and counter-notices			●	●
Special obligations for marketplaces, e.g. vetting credentials of third-party suppliers ("KYBC"), compliance by design, random checks			●	●
Bans on targeted adverts to children and those based on special characteristics of users			●	●
Transparency of recommender systems			●	●
User-facing transparency of online advertising			●	●
Risk management obligations and crisis response				●
External and independent auditing, internal compliance function and public accountability				●
User choice not to have recommendations based on profiling				●
Data sharing with authorities and researchers				●
Codes of conduct				●
Crisis response cooperation				●

Source: Europe fit for the Digital Age: new online rules for platforms. Accessed 26th April 2022.

Stakeholders

Intermediary service providers, recipients of the intermediary service

Main exclusions

Some exclusions intermediary services that are known as “mere conduit”, “caching” and “hosting” services and for micro and small enterprises.

4.3.4 Proposal for an Artificial Intelligence Act

Applies to artificial intelligence systems, which are defined as software that is developed with one or more of the techniques and approaches listed in Annex I of the proposed Act and can generate outputs such as content, predictions, recommendations, or decisions influencing the environments with which they interact.

Description

The AI Act aims to provide clarity around what can and cannot be done with artificial intelligence in the European Union. It established 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.

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.

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
Digital Markets Act	
To end unfair restrictions imposed by large-scale platforms, including cloud computing platforms, to reduce lock-in effects and increase innovation.	Inter alia[16], 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.
Digital Services Act	
Sets out obligations on intermediary information society services to ensure the proper functioning of the	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

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

internal market and a safe, predictable and trusted online environment in which the fundamental rights enshrined in the Charter are duly protected	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.
Artificial Intelligence Act:	
Proposes a single future-proof definition of AI and sets harmonised rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach.	Prohibited artificial intelligence practices include systems or services that, inter alia: • Use subliminal techniques to materially distort a person's 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[17] 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).

[17] Defined in Art. 6

	• 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. 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.

5.2 Defining key roles

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	Providers of on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised,

	Provider	distributed or highly distributed nature which includes cloud or edge computing platform providers but not content platform providers.
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.
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.

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
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.

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.
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).

6 CONCLUSIONS

6.1 The development of an NG-IoT roadmap

6.1.1 Investment and effort in the NG-IoT

The in-depth analysis of the SRIAs developed by the organisations that represent the European NG-IoT ecosystem reveals a diverse, rich and ambitious roadmap that covers research and innovation priorities across multiple domains and 146 distinct topics. Across the SRIAs, there are synergies that will help shape the future IoT:

Strategic drivers

- Sustainability as an end in itself, is a key driver for research and innovation across SRIAs and drive the development of a technology stack that is itself sustainable by design, planning for extended lifetime operation through mechanisms for:
    - Achieving reduced obsolescence
    - Component recyclability
    - Application of the technology to decarbonise and reduce energy consumption across industries
    - Low power sensors and devices, balancing power and performance
    - Improved thermal management
    - Efficient HPC.

Enablers

- Improvement of human-device interfaces to facilitate interaction and use of technologies, regardless of the skills level of the operator.
- Development of trust, not just at the technological level (ie. AI), but systemically across all applications and standards which incorporates changes in development and design of systems and the human-device interface.
- Actions that address market fit and readiness for the adoption of the technologies and applications.
- Orchestration of technologies that will underpin a federated cloud and data spaces, an updated role for the near edge.

Topics

- Most activity is directed at technology development *stricto sensu*, and standards, with little mention to skills.
- Relative to others, the Far Edge attracts the largest portion of attention in NG-IoT, with an emphasis on the development of new components and the creation of a network of intelligent devices.

Themes

- Contextual IoT is the most often mentioned theme, focusing on the need to address the deployment of IoT within constrained environments for trustworthy, relevant and autonomous/semi-autonomous decision-making. This is a complex topic, considering:
    - Operating within domain-specific models.

- Adapting to changes within the environment.
- Planning for and dealing with uncertainty and complex natural environments and
- Integrating multi-agent and human inputs.

- Interoperability continues to be a major concern, allowing for retro-fitting and integration with legacy infrastructure, assets and applications. It also acts as a mechanism to establish standards and approaches to engineering that will ultimately facilitate adoption across the whole value chain.

6.1.2 Possible gaps

Surprisingly, supply chain resilience did not seem to be a clear driver of research and innovation at the time the SRIAs were developed. Where the supply chain is mentioned, it is as a result of the research and innovation rather than the driving force behind it.

Edge nodes did not appear to be explicitly present in the SRIAs at the time this first report had been drafted, which may pose a risk to achieving the Digital Decade target of deploying 10,000 climate neutral highly secure edge nodes.

While the orchestration of devices is mentioned, the orchestration of container-based solutions that will enable the migration applications to the edge with context awareness is less evident at this stage. It is however, explicitly being addressed in the ICT 56 RIAs and has been included in the NG-IoT roadmap.

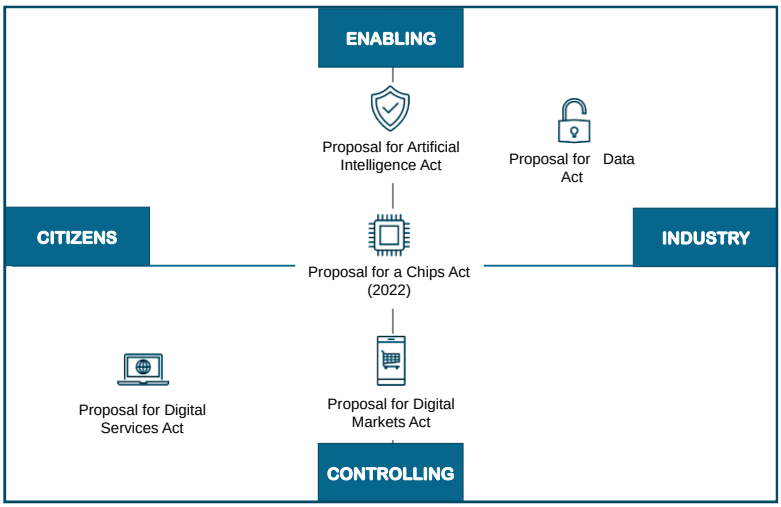
Nevertheless, it is difficult to determine the boundaries between the near and far edge and to confirm whether there is a gap that needs to be addressed. This, along with other topics will be explored in an expert workshop in Q3 2022.

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:



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 preceding regulations has the greatest relevance:

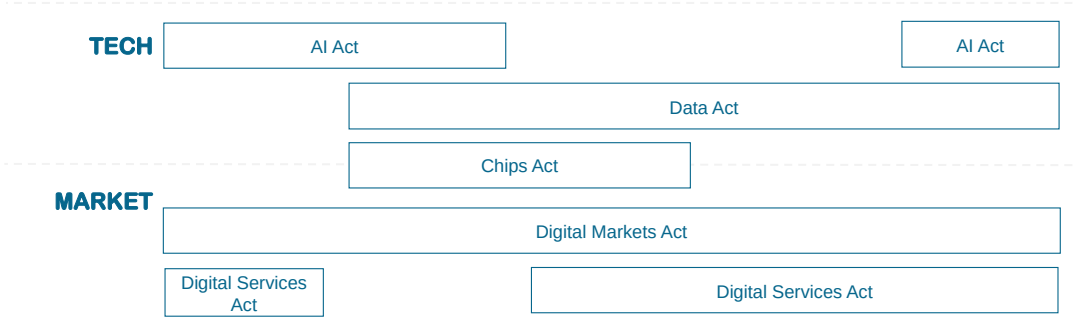


Figure 11. Mapping relevant regulation onto the NG-IoT

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[18].

[18] 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 –

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 stakeholders will be required to consider the design of their systems and architectures to provide the necessary functions and develop the 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 realtime biometric identification unless expressly allowed in the Act). high-risk AI systems[19] 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.

cannot be used as a reason for denying access to user-generated data.

[19] 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 CEI large scale-pilots can consider taking 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. [20]

   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[21] 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

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

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

functional equivalence. Future pilots could therefore explore interoperability standards that might support the portability of digital assets, and the opportunities and challenges that are opened up by the possible integration of multi-provider environments. 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[22] 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.

7.3 Supporting a future-proof CEI

1. VOLUNTARY CEI CODES OF CONDUCT

The proposed AI Act provides for voluntary codes of conduct that may be drawn up individual providers of AI systems or by organisations representing them with the involvement of users and stakeholders. There is an opportunity for future CSAs to support this process within and between different CEI communities.

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

2. TEMPLATES & TOOLS FOR CE MARKED AI

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.

3. STANDARDISATION TO OPERATIONALISE DATA SPACES

Across the Data Spaces operation, smart contract development and cloud interoperability, there is an opportunity to explore the development of European standards by the competent authorities and relevant SDOs. Common standards would help smart contracts, encouraging the development of automated data access interfaces and data spaces by industry.

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. Both regulators and public emergency bodies will have elevated and direct roles in the demonstrated platforms, solutions, and a significant interest in the outcomes which will reduce disruption for industry adoption of new obligations.

A regulatory sandbox created around the high-risk AI solutions to be developed will enable the upskilling of all stakeholders with managed learnings that will make solutions market-ready from the start and provide the dialogue between market regulators and tech developers which is a new ground outside of the Fintech sector.

Public agencies can also leverage the platforms in developing their own data capacities and technologies and acting as trials for future public interest tasks and examples of exceptional need.