Grant Agreement N°: 956671
Topic: ICT-56-2020

Shared Digital Future

Impact of key European legislation and proposals on the IoT and Edge community

Authors:
Tanya Suárez, Brendan Rowan, Martín Robles (BluSpecs)

The European IoT Hub

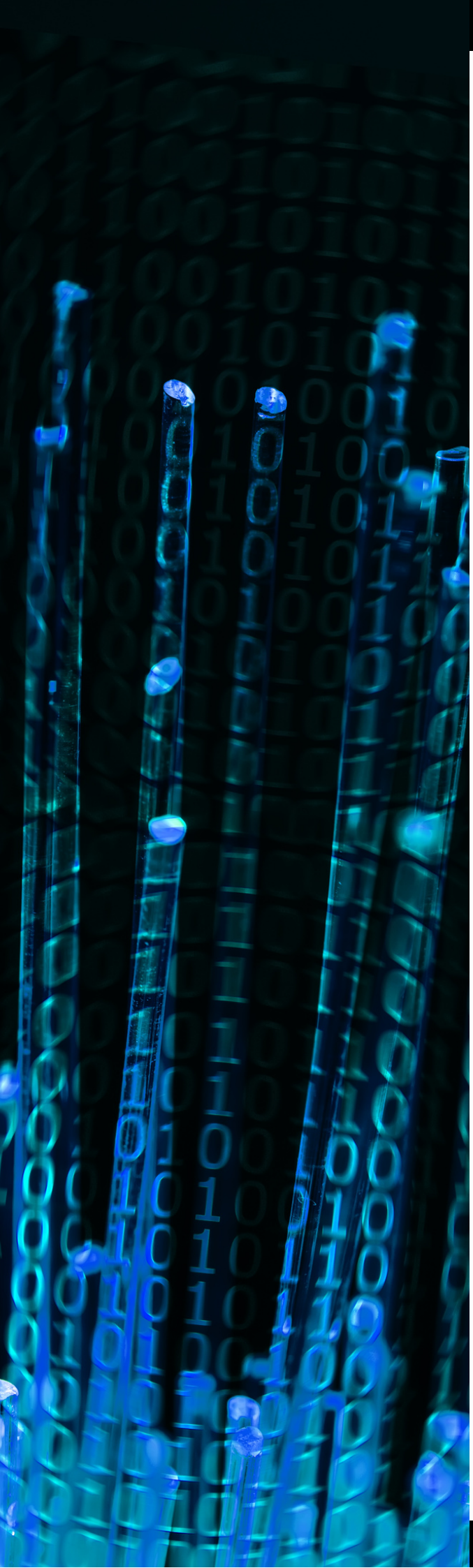
Growing a sustainable and comprehensive ecosystem for Next Generation Internet of Things

DISCLAIMER

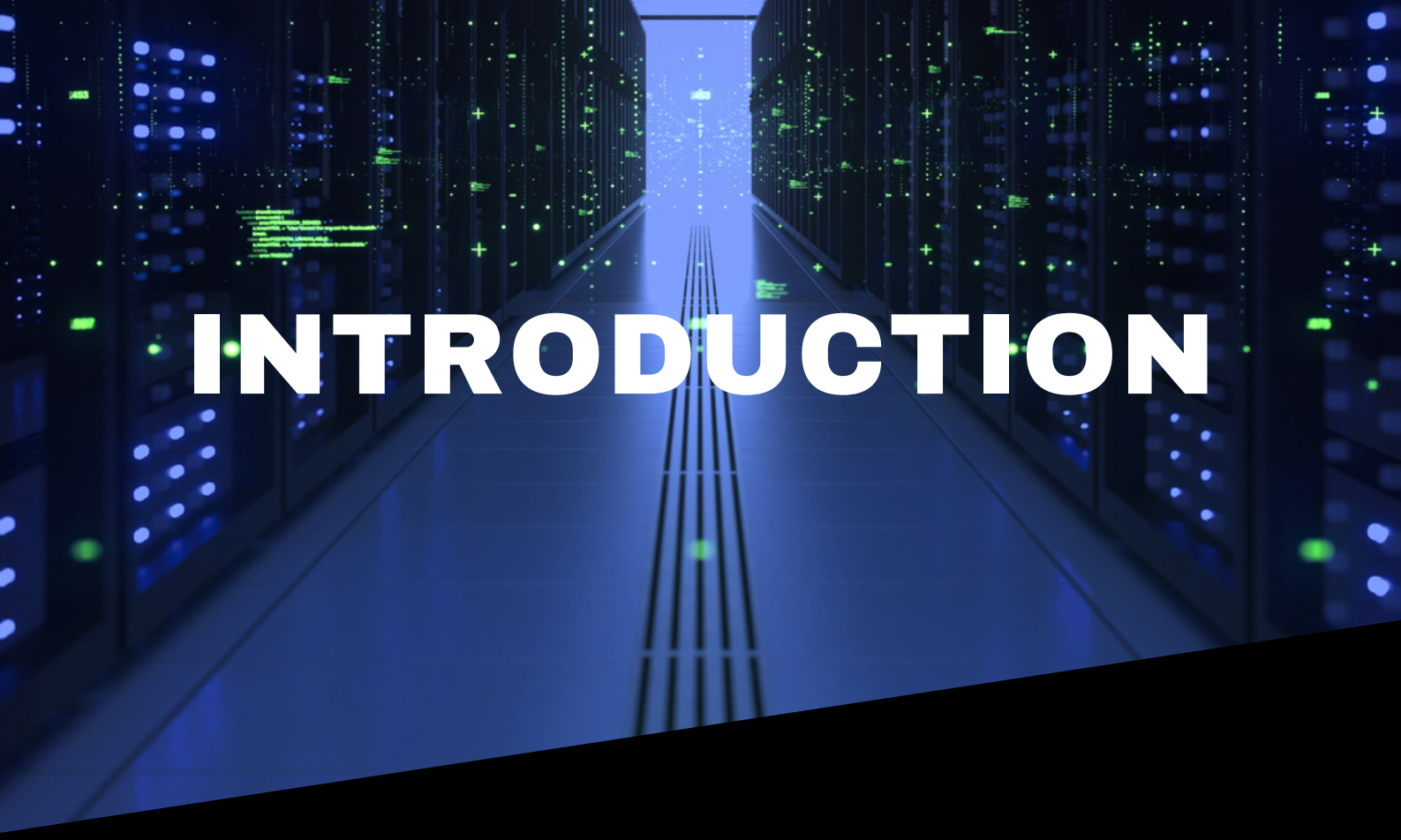
The information contained in this document is provided for informational purposes only and should not be construed as legal advice on any subject matter.
This information is:

- 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).

The content of this paper has been developed within the project EU-IoT, the Coordination and Support Action for the NGIoT Initiative funded by the European Union under Grant Agreement 956671. It does not reflect the views of the European Commission and as such the European Commission is not liable for any use that may be made of the information contained herein.



CONTENT



INTRODUCTION

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.

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.

INTRODUCTION

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; these include – but also go beyond – privacy, data protection, non-discrimination and access to justice.

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

European Agency for Fundamental Human Rights

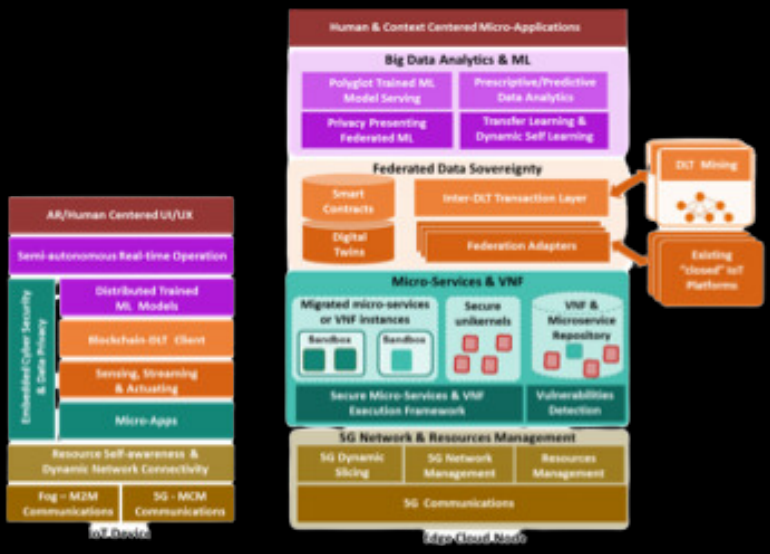
Getting the future right. Artificial intelligence and fundamental rights. 2020.

INTRODUCTION

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 Next Generation IoT?

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 are 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 function virtualisation and slicing.
- Management of public cloud and edge environments in the same application.



High-Level Next Generation IoT Archtecture
IoT_NGIN Consortium

EUROPEAN DIGITAL POLICY

The full impact of the ongoing 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* 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 those provided on the right. 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.

All regulations also confer 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.

- 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}

*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.

DATA ACT

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[1] 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.

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

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.

[1] P9_TA(2023)0069

DATA ACT

Exclusions, Principles and Limitations

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.

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

Excluded Data

- Data generated by prototypes.
- 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 ACT

Implications for the NGIoT

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."

CONNECTED PRODUCTS AND THEIR RELATED SERVICES MUST ENSURE THAT DATA GENERATED THROUGH USE IS ACCESSIBLE BY THE USER BY DEFAULT, EASILY, SECURELY.

DATA HOLDERS ARE REQUIRED TO PROVIDE DATA TO PUBLIC SECTOR BODIES AND AGENCIES TO RESPOND, PREVENT OR RECOVER FROM PUBLIC EMERGENCIES,

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 other cases.

SMEs are exempt from this obligation.

DATA ACT

Implications for the NGIoT

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.

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.

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.

DATA ACT

Implications for the NGIoT

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.

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 (eg. 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.

The specifications and European standards themselves 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 a 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.

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".

DATA ACT

Implications for the NGIoT

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.

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

SERVICE PROVIDERS MUST ENSURE THAT THEIR CUSTOMERS ENJOY FUNCTIONAL EQUIVALENCE IN THE USE OF THE NEW SERVICE.

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.

CYBER RESILIENCE ACT

Purpose, Scope and Exclusions

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
- Chip manufacturers
- Local authorities for cooperation and enforcement (still to be confirmed);
- European authorities: European Union Agency for Cybersecurity (ENISA)
- Consumers/users

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.

Implications for the NGIoT

CYBER RESILIENCE ACT

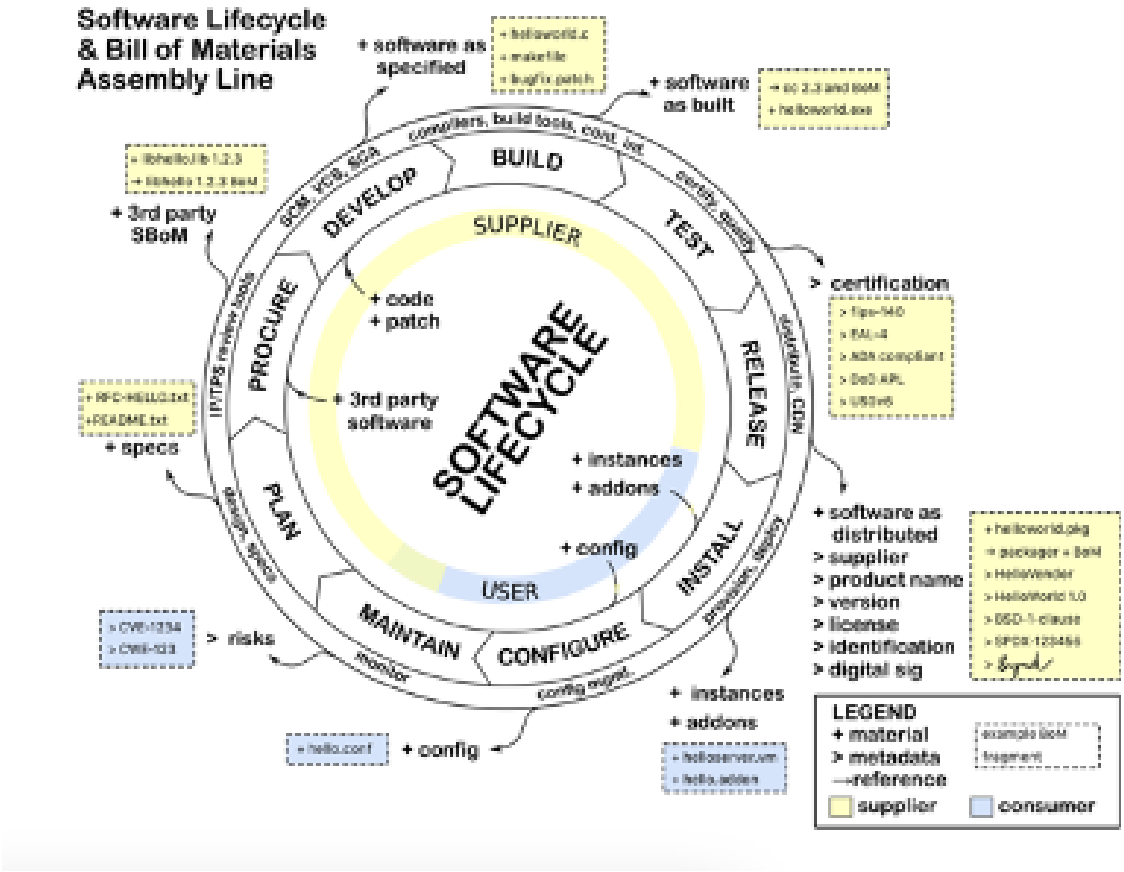
Increase in security throughout the NGIoT ecosystem

The increase of security throughout IoT ecosystem is an essential step towards the increase AI Trustworthiness, one of the strategic objectives across 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.



SBOM IN THE SOFTWARE CYCLE. SURVEY OF EXISTING SBOM FORMATS AND STANDARDS (2021) NTIA.

Implications for the NGIoT

CYBER RESILIENCE ACT

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[1].

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 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"[2] 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.

[1] AIOTI VIEWS ON THE CYBER RESILIENCE ACT, 2023
[2] P.18 2022/0272 (COD)

AI ACT

Purpose, Scope and Exclusions

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.

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.

Stakeholders

- Providers of AI systems in the EU;
- Users of AI systems located within the Union
- Poviders 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

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.

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.

AI ACT

Implications for the NGIoT

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”.

HIGH-RISK AI SYSTEMS REQUIRE ESTABLISHING, IMPLEMENTING AND DOCUMENTING A RISK MANAGEMENT SYSTEM.

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 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.

AI ACT

Implications for the NGIoT

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.

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.

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.

DIGITAL SERVICES PACKAGE

Purpose, Scope and Exclusions

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.

The DSA excludes services that are known as “mere conduit”, “caching” and “hosting” services; these beinginternet 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.

The DMA excludes electronic communications networks and electronic communications services as well as device manufacturers and software developers.

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 that act as gatekeeper. 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.

DIGITAL SERVICES PACKAGE

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.

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.

GATEKEEPER PLATFORMS 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.

IMPACT ON THE NGIOT

ACTIVELY REGULATING THE NGIOT

The development of a policy framework to guide the design, implementation, and deployment of technologies catering to Europe's citizens and businesses has become increasingly crucial.

Proposed regulations vary in scope and reach, with more restrictive provisions applied closer to the citizen level. Some regulations address existing market dominance problems and associated risks, while others aim to enable innovation by providing legal certainty and a future-proof operational framework.

SUMMARY

Implications for the NGIoT

Different regulations impact Next Generation Internet of Things (NG-IoT) building blocks to varying degrees. The AI Act and the Data Act are the most likely to have a direct, multi-faceted impact on the NG-IoT. The Data Act, in particular, will have significant implications for the Cloud-Edge-IoT Continuum, necessitating adjustments such as **defining data generation, usage, and accessibility in agreements**, and protecting SMEs through fair terms in data-sharing contracts.

The Data Act imposes obligations on cloud and edge platform operators, including enabling user switching and multi-vendor environments, developing mechanisms for **portability and functional equivalence**, and ensuring data security and integrity. It also defines the roles and responsibilities of data space operators, necessitating the design of systems and architectures with secure authentication and compliance features.

NG-IoT and Cloud-Edge-IoT (CEI) stakeholders must develop interoperability standards and smart contracts to overcome technical barriers and facilitate **authenticated data sharing**. "Minimum functionality" requirements need to be established through suitable standards and approaches, potentially driven by the European Telecommunications Standards Institute (ETSI) or similar organisations.

The proposed AI Act prohibits certain AI practices (e.g., real-time biometric identification) and mandates the establishment of risk management systems for **high-risk AI systems**. It requires specific provisions for training AI models with data, ensuring privacy and security, and monitoring for bias.

Additional provisions include generating technical documentation, recording events (logs), ensuring transparency, incorporating human-machine interfaces, and affixing the **CE marking** to indicate conformity.

The Act also encourages voluntary **Codes of Conduct** to address environmental sustainability, accessibility, stakeholder participation, and diverse development teams.

SUMMARY

Implications for the NGIoT

In summary, 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

The AI Act and Data Act, in particular, will have significant implications for stakeholders, requiring the development of interoperability standards, secure authentication features, and risk management systems. These regulatory efforts seek to provide a stable and future-proof framework for the development and deployment of NG-IoT technologies in Europe.

THE REGULATORY LANDSCAPE HAS ONLY JUST BEGUN TO ADAPT TO THE CHALLENGES OF A NEW DIGITAL & DATA FIRST ECONOMY.

THE NEXT-GENERATION IOT

THE NGIOT INITIATIVE

The NGIoT Initiative is a portfolio of 6 Research and Innovation Actions (RIAs) tasked with developing and trialling next-generation architectures. These NGIoT architectures 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.

The 48 million euro investment supported 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 work continues within the EU Cloud Edge IoT Continuum supporting cognitive cloud computing, metaOS development and swarm intelligence.

EU-IOT

The EU-IoT Coordination and Support Action aimed to transform the current IoT community of researchers and innovators in Europe into an increasingly cohesive, dynamic, participatory and sustainable ecosystem, as an essential part of a Next Generation Internet.

It provided a collaborative framework, including content, tools and processes, to engage all EU researchers, developers, integrators and users, fostering the creation of synergies, liaisons and exchange.

WWW.NGIOT.EU
WWW.EUCLOUDEDGE.EU

APPENDIX

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.

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.

RIGHTS AND OBLIGATIONS

Purpose	Main obligations
Data Act	
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, the customer achieves functional equivalence of the new services. • 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 standards 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.

RIGHTS AND OBLIGATIONS

Purpose	Main obligations
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.	• 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 ruless
AI 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.

RIGHTS AND OBLIGATIONS

Purpose	Main obligations
AI 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	Amongst other obligations, high-risk AI systems[1] 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.

RIGHTS AND OBLIGATIONS

Purpose	Main obligations
AI 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	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.

RIGHTS AND OBLIGATIONS

Purpose	Main obligations
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[1], 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.

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

RIGHTS AND OBLIGATIONS

Purpose	Main obligations
Digital Services Act	
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.

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 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 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.

KEY ROLES

Regulation	Key Figure	Definition
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.

KEY ROLES

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.
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).

KEY ROLES

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
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.

The European IoT Hub

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

FOLLOW US

WWW.NGIOT.EU

The EU-IoT work is partly supported by the European Union's Horizon 2020
Research and Innovation Programme (Grant Agreement no 956671).
Special thanks to all partners from the EU-IoT consortium and
to the EU-IoT Expert Group for valuable contributions.