

IoT Guide: Global IoT Regulations



Contents

1. Introduction	3
2. Hardware and spectrum	7
2.1 Device certification	7
2.2 Import and export controls, including for tax purposes	8
2.3 Environmental regulations related to disposal of devices	8
2.4 RF regulations	9
2.5 Product safety standards	9
2.6 Energy Efficiency Standards	9
3. Licensing and permanent roaming	11
4. Privacy	17
5. Security	21
6. Data sovereignty and access/portability	27
7. National resilience	31
8. Regulations in vertical sectors	33
8.1 Consumer electronics	33
8.2 Automotive	33
8.3 Financial services	34
8.4 Utilities	34
8.5 Healthcare	35
8.6 Drones	35
8.7 Supply chain	35
8.8 Lone worker safety	36
8.9 Environment	36
8.9.1 Smart buildings	37
9. Conclusions and recommendations	39



01

Introduction

Introduction

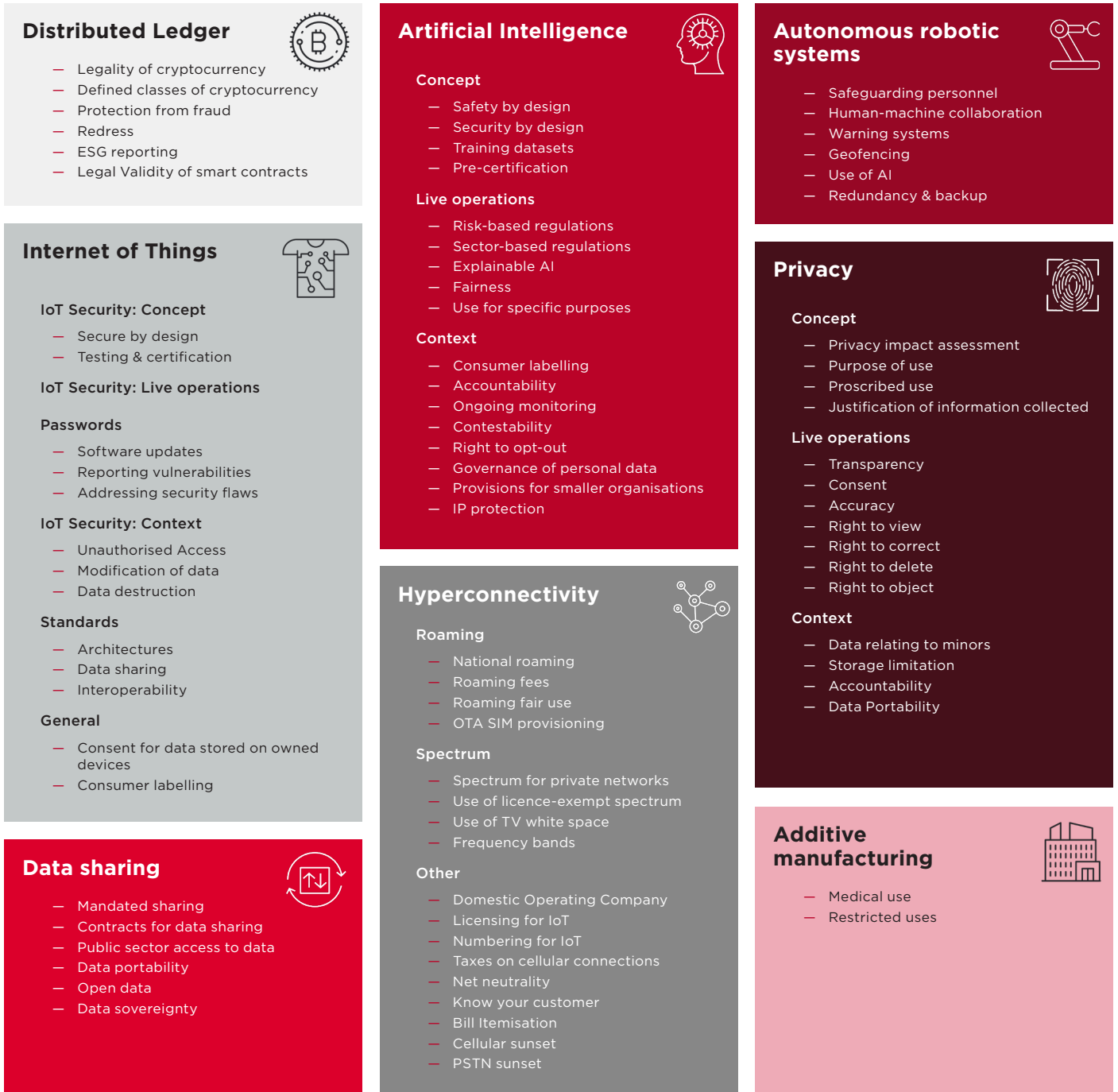
This report provides a guide to the various regulations that affect deployments of the Internet of Things and the associated provision of connectivity, device functionality, and management of data, as well as regulatory drivers and barriers to adoption.

The report draws heavily from the Transforma Insights Regulatory Database, which details the key aspects of regulations (the 'DNA of Regulations') that apply in a range of new and emerging

technology domains, such as the Internet of Things, Hyperconnectivity, Artificial Intelligence, Data Sharing, Distributed Ledger, Additive Manufacturing, and Autonomous Robotic Systems. A further domain relates to Privacy, which will often need to be considered alongside any technology-specific regulations.

The key areas of regulation contained within the Regulatory Database are highlighted in the figure below.

Figure 1
The DNA of Regulations for Digital Transformation










Source: Transforma Insights, 2023

This report pulls together and summarises those areas related to the Internet of Things, as well as filling out the spectrum of regulation by covering some of the more mundane and well-established

regulations. More detail can be found in the database. It compiles the regulations into seven major areas.

Figure 2

Seven areas of regulation relevant to IoT

<p>1 Hardware and spectrum</p> 	<p>There are many long-standing regulations related to factors such as RF regulations, device certification and product safety which are relevant to IoT. Recent years have seen a flurry of regulations related to energy efficiency and sustainable disposal. We also consider import/export controls.</p>
<p>2 Licensing and permanent roaming</p> 	<p>Relates specifically to the provision of public networks (most usually cellular networks) and very specifically the restrictions that might apply to extra-territorial use of E.164 number (otherwise known as 'permanent roaming'),</p>
<p>3 Privacy</p> 	<p>Some of the first regulations affecting IoT data were those related to data privacy more broadly, which address the collection, storage, and processing of personal data. This includes the EU GDPR regulation and various consumer privacy regulations around the world.</p>
<p>4 Security</p> 	<p>The last few years have seen a major expansion in the amount of legislation related to cybersecurity. In general and IoT device security particularly. There are also numerous examples of codes of practice pertaining to cybersecurity topics such as passwords and firmware updates.</p>
<p>5 Data sovereignty and access/portability</p> 	<p>Many countries have particular rules about the circumstances in which data may or may not be accessed by government, shared within countries and sent overseas. This includes the US CLOUD Act and various EU regulations such as the Data Act and the Data Governance Act.</p>
<p>6 National resilience</p> 	<p>As a further evolution on the requirements for device security and data sovereignty, an increasing number of countries are implementing stricter rules related to national resilience and protection of critical national infrastructure (CNI), including rules around procurement.</p>
<p>7 Regulations in vertical sectors</p> 	<p>As well as the general regulations related to IoT and associated fields outlined under the headings above, there are also numerous vertical-specific regulation which can also be relevant for IoT, including in automotive, energy, financial services and the public sector.</p>

Source: Transforma Insights, 2024

This is not an exhaustive list of all regulations that might apply to IoT deployments.

The report also provides guidance on best practice for IoT vendors and adopters related to compliance.

In the following sections we identify the variety of key regulations, including some key examples from specific countries, related to the Internet of Things which can be divided into several main categories as outlined above.



02

Hardware and spectrum

Hardware and spectrum

There are a number of regulations that companies providing IoT services will need to comply with related to IoT hardware and how devices access telecommunications networks.

2.1

Device certification

The aim of device certification is to ensure that IoT devices do not create problems for the networks upon which they will reside, for instance by using up unnecessary amounts of network resources or potentially causing network outages.

In some cases this certification is required by government regulation. Examples of such government regulations include:



Brazil – Agência Nacional De Telecomunicações (Anatel), the Brazilian telecoms regulator, certifies telecommunications terminal equipment as well as network infrastructure. Certification is done by a Designated Certification Body.



China – IoT devices are required to comply with China Compulsory Certification (CCC). The full CCC is a mandatory certification which involves product testing and inspection. The CCC framework also includes a range of self-declaration and voluntary declarations for certain device types.



EU – Electromagnetic Compatibility (EMC) Directive and Radio Equipment Directive – Regulations for certain device types, particularly connected devices, related to ensuring that devices will not interfere with – or be at risk of being interfered with by – other radio equipment.



India – According to the guidelines in the Indian Department of Telecommunications (DoT) ‘Registration Process of M2M Service Providers (M2MSP) and WPAN/WLAN Connectivity Providers for M2M Services’ a registrant shall induct only those devices/equipment in the network which meet TEC standards and certifications.



Saudi Arabia – The country’s IoT framework includes rules that IoT equipment obtain a Certificate of Conformity before applying for customs clearance.

In other cases, the certification requirements are set by the mobile industry. For instance, in the US, mobile network operators (MNOs) generally require a device be certified with the PTCRB (PCS Type Certification Review Board) before accepting devices onto their networks. Another example of a common certification body is the Global Certification Forum (GCF), which was established by MNOs and mobile device manufacturers. It certifies through Recognised Test Organisations (RTOs) based on test specifications from standards development organisations in the telecommunications sector, such as 3GPP. Mobile operator – separate certification related to RF performance, for instance. Additional to these common certifications, some MNOs will have further specific certification requirements.

2.2

Import and export controls, including for tax purposes.

Some national regulations restrict either the export or import of some categories of IoT devices, although often only in exceptional cases:



United States - The United States Bureau of Industry and Security (BIS) administers export controls on certain IoT devices under the Export Administration Regulations (EAR). Items classified under the EAR may require a license for export, depending on factors such as destination country, end-user, and intended use.



European Union - The European Union regulates the export of certain IoT devices through the EU Dual-Use Regulation, which controls the export of goods, software, and technology that can have military as well as civilian applications.



China - China imposes import and export controls on IoT devices through various regulations administered by agencies such as the Ministry of Commerce (MOFCOM) and the State Administration for Market Regulation (SAMR).



Australia - The Australian Border Force (ABF) administers import controls on IoT devices entering the country, ensuring compliance with regulations related to safety, security, and standards.



Canada - Canada's Export Controls Division, part of Global Affairs Canada, regulates the export of IoT devices under the Export and Import Permits Act (EIPA) and the Export Control List (ECL), which identify controlled goods and technologies.



South Korea - South Korea's Ministry of Trade, Industry and Energy (MOTIE) regulates the import and export of IoT devices through various laws and regulations, including the Foreign Trade Act and the Act on the Prevention of Divulgence and Protection of Industrial Technology.

2.3

Environmental regulations related to disposal of devices.

Several jurisdictions have rules related to e-waste and the sustainable disposal of electronics devices. These include:



European Union - The Waste Electrical and Electronic Equipment (WEEE) Directive requires member states to establish collection and recycling systems for electronic waste, including IoT devices, to minimize their environmental impact.



United States - The Resource Conservation and Recovery Act (RCRA) regulates the disposal of electronic waste, including IoT devices, by imposing requirements on their treatment, storage, and disposal to prevent environmental contamination.



Japan - The Act on the Promotion of Recycling of Small Waste Electrical and Electronic Equipment requires manufacturers to establish recycling programs for small electronic devices, including certain types of IoT devices.



South Korea - The Act on Resource Circulation of Electrical and Electronic Equipment and Vehicles regulates the recycling and disposal of electronic waste, including IoT devices, to promote resource conservation and environmental protection.



India - The E-Waste (Management and Handling) Rules require producers, consumers, and recyclers of electronic waste, including IoT devices, to comply with regulations for their environmentally sound management and disposal.



China - The Regulations for the Administration of the Recovery and Disposal of Waste Electric and Electronic Products require manufacturers, importers, and retailers to take responsibility for the recycling and disposal of electronic waste, including IoT devices.

2.4

RF regulations

The use of radio spectrum is licensed by regulatory bodies such as the Federal Communications Commission (FCC) in the US, Ofcom in the UK, or the Bundesnetzagentur (Federal Network Agency) in Germany. These bodies set licensing requirements for access to licensed spectrum.

Regulatory bodies such as the FCC and standards organisations such as the European Telecommunications Standards Institute (ETSI) set standards for the use of radio frequencies by IoT devices to avoid interference with other wireless technologies. Typically, rules cover topics such as access to unlicensed spectrum (including rules over duty cycle and power output) and issue of incompatible spectrum allocations for unlicensed devices.

For instance, in the EU, the Radio Equipment Directive (2014/53/EU) sets harmonized rules for the placing of radio equipment on the market within the EU. IoT devices that incorporate radio communication capabilities, such as Bluetooth, Wi-Fi, or cellular connectivity, must comply with the requirements of the RED, including

conformity assessment, CE marking, and compliance with essential requirements related to safety and electromagnetic compatibility (EMC).

2.5

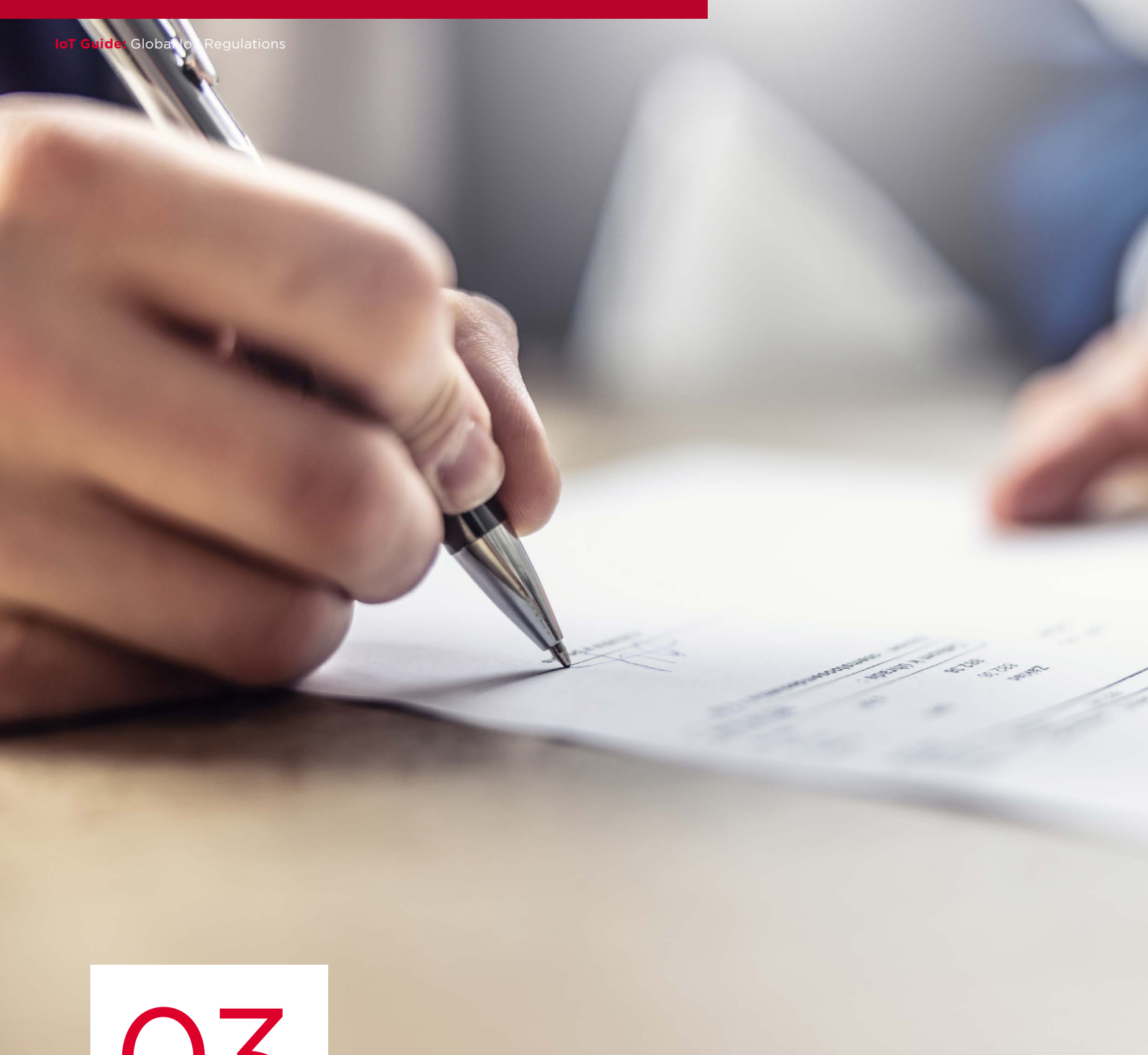
Product safety standards

Regulations like the CE marking in the European Union and FCC certification in the United States establish safety requirements for IoT devices to ensure they do not pose risks to users or the environment.

2.6

Energy Efficiency Standards

Some regions have regulations and standards promoting energy efficiency in IoT devices to reduce their environmental impact and energy consumption. For instance the Energy Efficiency Directive (2012/27/EU) sets targets for improving energy efficiency across various sectors, including buildings, transport, and industry. IoT devices, particularly those used in smart buildings, smart grids, and industrial automation, can contribute to energy savings and must comply with relevant energy efficiency requirements and standards.



03

Licensing and permanent roaming

Licensing and permanent roaming

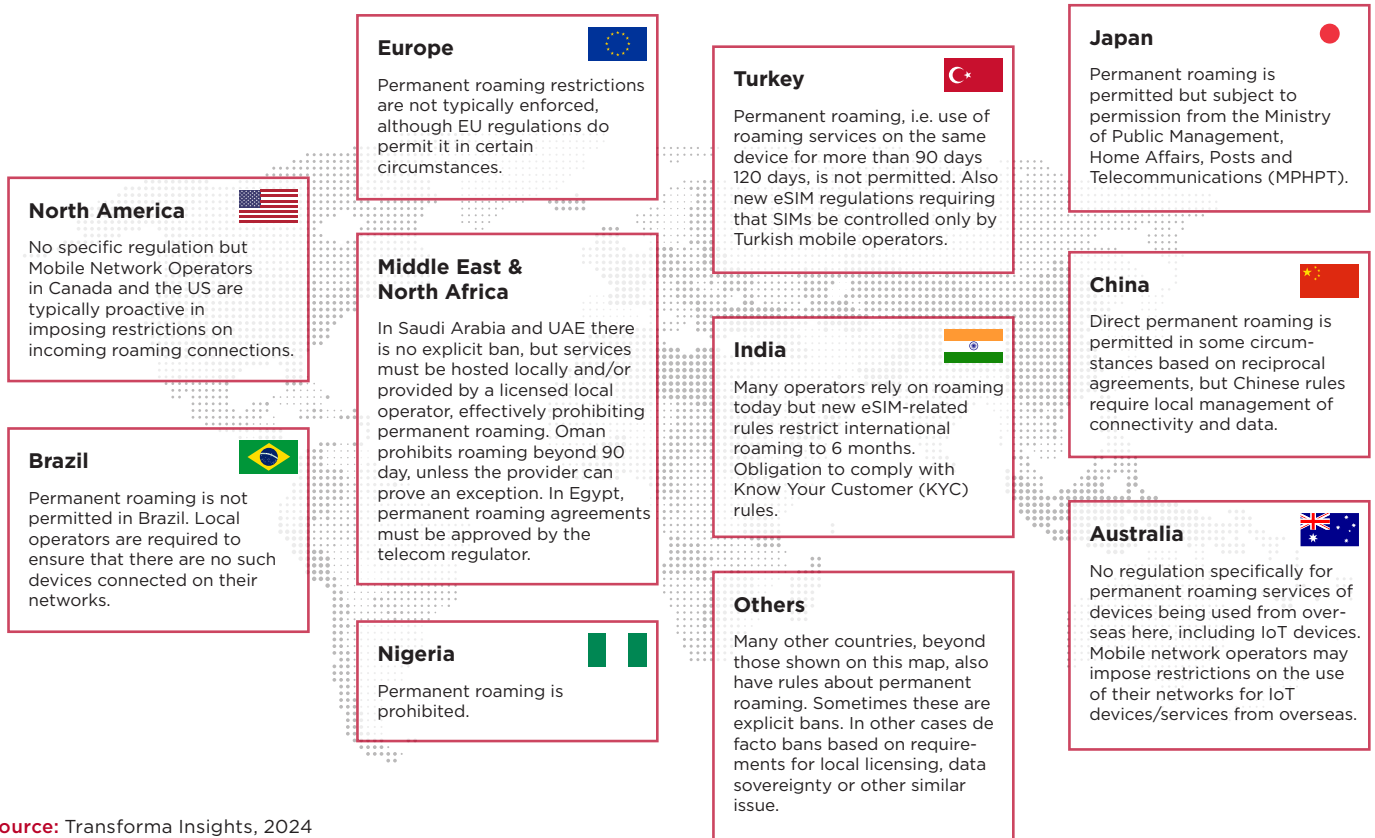
As well as the general rules related to devices connecting to telecommunications networks there are also specific rules about which companies can provide IoT connectivity services in various markets. Typically these relate to the licensing of operators, including requirements for registration with arbitration services, support for lawful intercept, provision of location information for emergency services and 'know your customer' (KYC) rules.

One particularly relevant set of regulations for supporting IoT relates to extra-territorial use of E.164 number (which is generally referred to as 'permanent roaming'). Many, perhaps most, IoT deployments using cellular connectivity involve connecting devices in multiple countries. Many have specific rules about how that connectivity is supported, in particular whether cellular-connected devices could exist in a state of 'permanent roaming', i.e. a device that is connected by a connectivity provider that is not licensed in the territory could use its roaming agreements with licensed operators to support a connection that was not simply temporarily roaming but would be present on a permanent basis in that country.

During the 2010s many regulators, for instance in Brazil, China, India and Turkey, introduced, or more rigorously enforced, rules that prohibited permanent roaming. Sometimes the rules were explicitly against permanent roaming and in other cases were based on local registration requirements or tax obligations. The regulators are often motivated to protect the local market and enforce local rules with which a roaming connection may not comply, e.g. lawful intercept. Besides this, roaming was never envisaged to include a foreign device permanently being in a state of roaming.

There were also commercial equivalents, particularly in the US and Canada, where the operators themselves prohibited their roaming partners from having devices permanently roaming on their networks. In this section we discuss the regulations (or commercial equivalents) that explicitly or implicitly prohibit permanent roaming in countries around the world. Permanent roaming covers a range of scenarios, from that related to licensing, taxation, rules on management of eSIM localisation, or KYC rules, all of which can act to effectively prohibit the practice. In many cases the issue relates to licensing, i.e. the company providing the services needs to be based on the country. Hence there is a lot of overlap between the two topics.


Figure 3
Permanent roaming rules



Source: Transforma Insights, 2024

The list below provides a summary of some of the main rules related to permanent roaming in various countries:

-  **Australia** – The Australian Communications and Media Authority (ACMA) doesn't have regulation specifically for permanent roaming services of devices being used from overseas here, including IoT devices. Mobile network operators may impose restrictions on the use of their networks for IoT devices/services from overseas.
-  **Brazil** – Local telecommunications regulator Anatel prohibits permanent roaming.

-  **Canada** – There are no regulatory prohibitions on permanent roaming, although the MNOs can and do implement their own restrictions on specific roaming operators.
-  **China** – Permanent roaming is permitted in some circumstances, but Chinese rules require that data and connectivity be managed locally in country.
-  **Egypt** – Usage of permanent roaming requires a signed agreement between the foreign operator of the SIM installed in the IoT device and a national mobile operator

in Egypt. The agreement needs to be approved by the National Telecom Regulatory Authority (NTRA) of Egypt.



European Union – Permanent roaming rules are not typically enforced, although EU regulations do permit it in certain circumstances. Regulation 2022/612 on roaming on public mobile communications networks within the Union provides for a common approach for ensuring that users of public mobile communication networks, when travelling within the Union, do not pay excessive prices. It lays out that mobile network operators (MNOs) shall meet all reasonable requests for wholesale roaming access, in particular in a manner that allows the roaming provider to replicate the retail mobile services offered domestically where it is technically feasible to do so on the visited network. MNOs may refuse requests for wholesale roaming access only on the basis of objective criteria, such as technical feasibility and network integrity, not commercial considerations. MNOs shall publish a reference offer which may include conditions to prevent permanent roaming or anomalous or abusive use of wholesale roaming access.



India – Currently many global connectivity providers use permanent roaming but the regulatory situation is set to change. The Telecom Regulatory Authority of India (TRAI) had previously recommended that a period of 3 years of permanent roaming was acceptable. However, it issued a set of recommendations in March 2024 that stated: “All communication profiles on any M2M eSIM fitted in an imported device on international roaming in India should be mandatorily converted/reconfigured into communication profiles of Indian telecom service providers (TSPs) within a period of six months from the date of activation of international roaming on such M2M eSIM or on change of ownership of the device, whichever is earlier.” The same restrictions also apply to MCC-901 IMSIs. Those devices supported with a local IMSI are therefore assumed to be compatible. Additionally rules about Know-Your-Customer (KYC) also apply.



Japan – Permanent roaming is permitted, but with a requirement for registration. In the case of Special Type II telecommunications carriers, where intending to conclude a roaming contract with a foreign carrier, an MVNO shall obtain approval from the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) and where an MVNO provides service for foreign carrier’s terminals within Japan, a relevant MNO shall obtain permission for operation from the MPHPT.



Jordan – We understand that the use of permanent roaming in Jordan requires a signed agreement between any foreign operator that owns a SIM card and the national mobile operator that supports roaming.



Kuwait – We understand that no specific rules or frameworks apply for IoT services and these services are only subject to the regular licensing frameworks of non-IoT telecommunications services.



Lebanon – We understand that no specific rules or frameworks apply for IoT services and these services are only subject to the regular licensing frameworks of non-IoT telecommunications services.



Morocco – We understand that no specific rules or frameworks apply for IoT services and these services are only subject to the regular licensing frameworks of non-IoT telecommunications services




Nigeria – Permanent roaming is prohibited.



Oman – The Telecommunications Regulatory Authority issued a directive on IoT devices using international roaming. The directive targets those licensed to provide Internet of Things services, service providers, suppliers, and integration service providers, and seeks to regulate international roaming for Internet of Things devices, enhance the security level of Internet of Things services provided to beneficiaries, and protect their personal data. The directive states that the provider or importer can provide Internet of Things devices with international roaming services or via local



networks, provided that international roaming operates on a temporary basis in accordance with a number of obligations, namely that the Internet of Things devices operate using the subscriber identification card (SIM/E-SIM) from the licensor. They will be allowed to use international roaming SIM cards for these devices in the Sultanate of Oman for a period not exceeding 90 days in local networks. Suppliers or importers of Internet of Things devices operating in international roaming, if they wish to extend it for more than 90 days, can apply to the Authority to request an exception and the justifications for that to be studied and decided on via the Authority's website.

 **Qatar** - We understand that no specific rules or frameworks apply for IoT services and these services are only subject to the regular licensing frameworks of non-IoT telecommunications services.

 **Saudi Arabia** - In September 2019, Saudi Arabia's Communications and Information Technology Commission (CITC) published an IoT Regulatory Framework. Amongst other things, the framework required that IoT services through mobile networks can be provided only by licensed

service providers from the CITC, such as Facilities Based Unified Licensees, MVNOs, IoT-VNOs, or any other licenses as defined by CITC.



Singapore - Permanent roaming is permitted, with the only limit being that the seller of IoT equipment is required to apply for a telecommunications dealer licence and may need to acquire a services licence. Furthermore there are rules about the devices in which the SIMs sit, specifically the need to comply with standards and meet the Infocomm Media Development Authority (IMDA) approval process.



Switzerland - There are no legal obligations for IoT service providers to register with local authorities and no other restrictions on permanent roaming.




Tunisia - We understand that no specific rules or frameworks apply for IoT services and these services are only subject to the regular licensing frameworks of non-IoT telecommunications services.





Turkey - Permanent roaming is not allowed in Turkey. According to Turkish Law 7186-23 permanent data roamers will be banned from Turkish MNO networks.

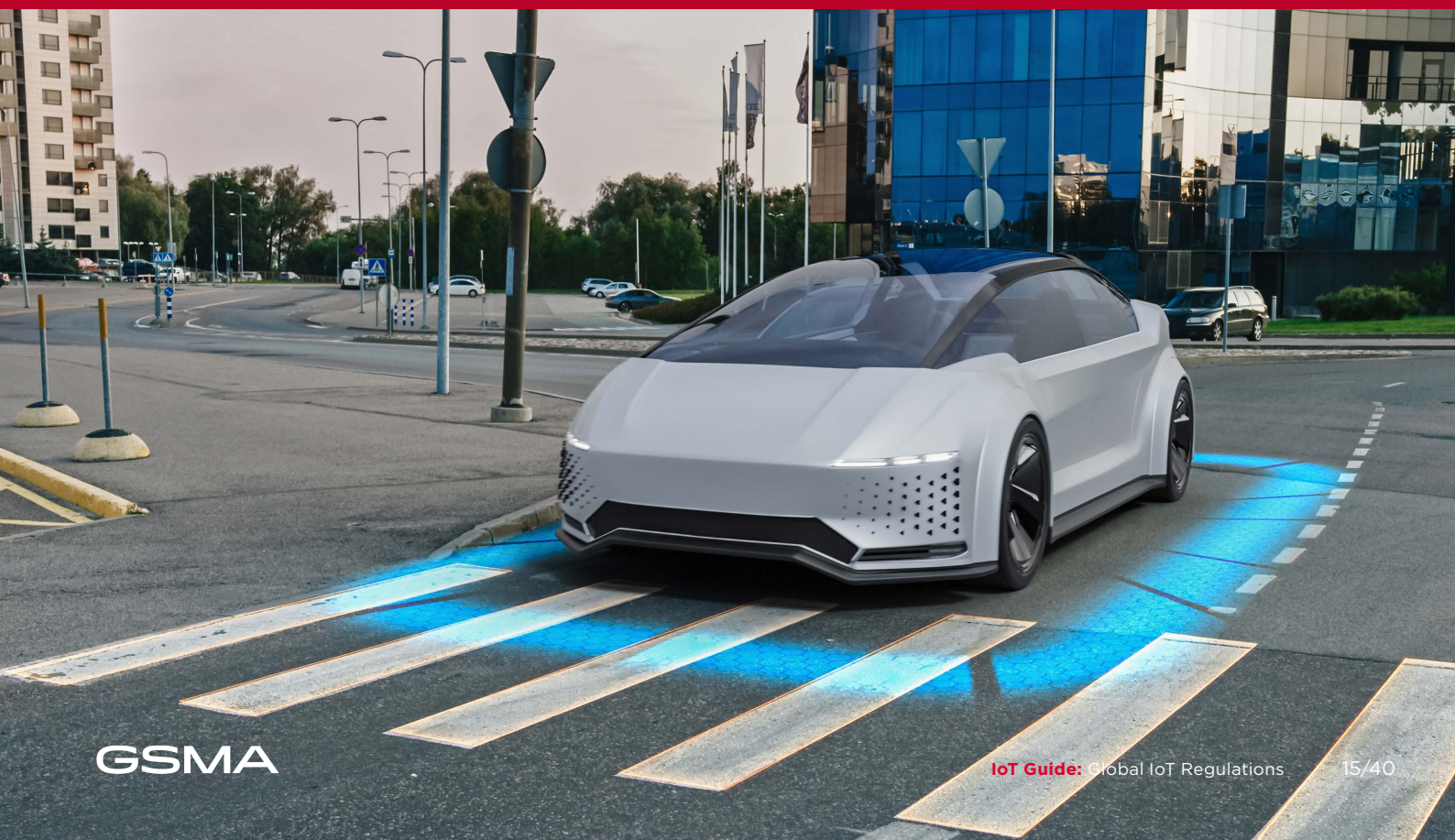
Furthermore, Turkey's regulation around Remote Programmable SIM Technologies requires that the SIM needs to be controlled only by mobile operators in Turkey and that only mobile operator profiles from Turkey can be uploaded. All structures, systems and storage units, including software, must be operated by an operator authorized in Turkey or by an approved third party determined by the operators.

 **UAE** - For provisioning of IoT services via embedded non-UAE SIM Cards, as per the TDRA regulation the sale of SIM cards in the UAE is regarded as a Regulated Activity and requires a Telecommunications License. However, to enable legacy IoT services in the UAE, the TDRA has on an exceptional interim basis allowed the provisioning of IoT solutions provided via embedded non-UAE SIM cards, subject to there being a roaming agreement in place with a UAE Licensee and subject to any/all data being stored in the UAE. The exceptional allowance of non-UAE embedded SIM cards is however only an interim solution and the TDRA is expecting the IoT provider's compliance with the regulatory framework and any requirements

from the competent Authorities. Hence the TDRA is expecting the IoT service providers to urgently migrate all current and all legacy embedded SIM cards to UAE programmable SIM solutions to ensure the requirements of UAE profiles. The TDRA is expecting to prohibit the usage of non-UAE embedded SIM cards that cannot be utilized with a UAE profile in the near future. Also, the TDRA is expecting the IoT service providers to host locally in the UAE the servers used to store/process the data in the near future.

 **UK** - There are no specific regulations around permanent roaming although providers of telecommunications services need to register with the UK regulator.

 **US** - There are no regulatory prohibitions on permanent roaming, although the MNOs can and do implement their own restrictions on specific roaming operators.





04

Privacy

Privacy

Some of the first regulations affecting IoT data were those related to data privacy more broadly, which address the collection, storage, and processing of personal data. Examples of rules related to privacy include:

- 

EU – General Data Protection Regulation (GDPR): Enforced in the European Union, GDPR sets rules for the collection, processing, and storage of personal data, including data collected by IoT devices. It requires explicit user consent, transparent data practices, and mechanisms for data subjects to access and control their information. Additionally, the ePrivacy Directive (2002/58/EC) complements GDPR by focusing on privacy and electronic communications. It regulates the processing of personal data in the context of electronic communications services, including IoT devices such as smart meters and connected appliances.

manufacturers and service providers. It emphasizes consent, accountability, and transparency in data handling practices.
- 

US – California Consumer Privacy Act (CCPA): California’s privacy law grants consumers in the state rights over their personal information collected by businesses, including IoT devices. It requires businesses to disclose data collection practices, provide opt-out mechanisms, and refrain from selling personal information without explicit consent.



Singapore – Personal Data Protection Act (PDPA): PDPA establishes rules for the collection, use, and disclosure of personal data, including data obtained through IoT devices. It requires organizations to obtain consent, implement data protection measures, and provide individuals with rights over their data.
- 

Canada – Personal Information Protection and Electronic Documents Act (PIPEDA): PIPEDA regulates the collection, use, and disclosure of personal information by private sector organizations, including IoT device



China – Personal Information Protection Law (PIPL): PIPL, effective as of 2021, governs the processing of personal information by organizations, including IoT device manufacturers and operators. It requires lawful and legitimate data processing, explicit consent, and protection of individuals’ rights.
- 

Australia – Privacy Act of 1988: Australia’s privacy law regulates the handling of personal information by Australian government agencies and certain private sector organizations. It requires compliance with privacy principles, including transparency, data security, and individual rights, in the context of IoT data collection and processing.



Malaysia – Personal Data Protection Act (PDPA): DPA regulates the processing of personal data by businesses, including IoT service providers and device manufacturers. It mandates consent, data accuracy, security safeguards, and accountability in handling personal information.



Brazil – Lei Geral de Proteção de Dados (LGPD): Inspired by GDPR, LGPD regulates the processing of personal data by public and private organizations, including data collected through IoT devices. It emphasizes consent, transparency, security, and accountability in data processing practices.



India – Data protection provisions for consumer IoT require that the manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to any involved third parties, including advertisers. Where personal data is processed based on consumers' consent, this consent shall be obtained in a valid way.

Obtaining consent “in a valid way” normally involves giving consumers a free, obvious, and explicit opt-in choice of whether their personal data can be used for a specified purpose.

Obtaining consent “in a valid way” normally involves giving consumers a free, obvious, and explicit opt-in choice of whether their personal data can be used for a specified purpose. Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time. Consumers should be able to preserve their privacy by configuring IoT devices and service functionalities appropriately.

As well as these general privacy regulations there are often also specific rules related to data created for certain use cases or sections of the population. For instance, the Health Insurance Portability and

Accountability Act (HIPAA, see the 'Regulation in vertical sectors' section, below) or the Children's Online Privacy Protection Act (COPPA), which regulates the collection of personal information from children under the age of 13.

There are also compliance frameworks relevant to both security (see the 'Security' section, below) and privacy such as the Service Organization Control Type 2 (SOC2) developed by the American Institute of Certified Public Accountants (AICPA) which include best practice related to the management of personal customer data.

As well as these general privacy regulations there are often also specific rules related to data created for certain use cases or sections of the population.





05

Security

Security

The last few years have seen a major expansion in the amount of legislation related to cybersecurity in general and IoT device security particularly. The regulations presented below represent the most significant cybersecurity rules and guidelines related to IoT. Many other countries will have similar rules.

There are numerous examples of codes of practice or guidelines for minimum levels of security on consumer IoT devices, including for instance not using default or weak passwords, and requirements for regular firmware updates. In some countries these voluntary guidelines have been replaced by mandatory requirements and this trend is likely to continue. Other elements include labelling programmes.

The list below presents just a summary of the regulations and codes of practice.



Australia - In September 2020, the Department of Home Affairs in Australia, in partnership with the Australian Signals Directorate's Australian Cyber Security Centre published its '**Code of Practice: Securing the Internet of Things for Consumers**' to enhance the cyber security of internet-connected devices. The Code of Practice constitutes a voluntary set of principles and compliance with these principles is encouraged but optional. The Code of Practice comprises thirteen principles, including not to using default or weak passwords, secure storage of credentials, protection of personal data, maintaining a vulnerability disclosure policy, and minimum security update requirements.



Brazil - In January 2021, Brazil's National Telecommunications Agency published its **Cybersecurity Requirements for Telecommunications Equipment** which required that, amongst other things, devices have automated and secure mechanisms for updating software/firmware, allow users to manually check for availability of software/firmware updates and easily deploy them, have mechanisms to inform the user of software/firmware changes implemented due to updates, have a mechanism for monitoring unusual software/firmware behaviour, protect stored or transmitted passwords, access keys, and credentials using appropriate encryption or hashing methods, and allow users to easily delete their stored personal and sensitive data.



China - In September 2021, the Ministry of Industry and Information Technology (MIIT) in China published **Guidelines for the Development of the Internet of Things Basic Security Standard System (2021 Edition)**. The guidelines lay down five standards for a basic IoT security standard system including overall security (including basic definitions and architecture models), terminal security (including relating to authentication and testing), gateway security, platform security (for device management, connectivity management, application enablement platform and others), and security management.




EU - The EU has several regulations related to cybersecurity. In recent years the EU has focused a lot of attention on cybersecurity as well as having a very active strategy related to data (see 'Data sovereignty and access/portability' section, below).




- On December 9, 2020, the European Union Agency for Cybersecurity (ENISA), published **guidelines for securing the supply chain for IoT**. ENISA created security guidelines for the whole lifespan, including requirements, design, end use delivery, maintenance, disposal, etc. The study aims to help IoT manufacturers, developers, integrators, and all stakeholders that are involved to the supply chain of IoT to make better security decisions when building, deploying, or assessing IoT technologies. The guidelines presented good practices to consider such as prioritising working with suppliers that provide cybersecurity guarantees, adopting the view of security in the supply chain as a continuous process, favouring the adoption of SLAs that require the presence of software integrity measures, and providing security promises to customers. The document lays down good practices to provide a safe and secure product, including adopting secure-by-design principles, implementing mechanisms for remote updates, requiring factory settings that use security by default, providing Software Bill of Materials (SBOMs) for IoT devices, and committing to provide security patches.
- In September 2022, the European Commission proposed a regulation on cybersecurity requirements for products with digital elements, known as the **Cyber Resilience Act**. The Act intends to bolster cybersecurity rules to ensure more secure hardware and software products. The proposed regulation states that products with digital elements shall be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks. When placing a product with digital elements on the market and for the expected product lifetime or for a period of five years from the placing of the product on the market (whichever is shorter), manufacturers shall ensure that vulnerabilities of that product are handled effectively.
- The **Network and Information Security (NIS) Directive** was the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high, common level of cyber security across the Member States. To respond to the growing threats posed by digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to


replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by **NIS2**, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. It entered into force on 16 January 2023, and the Member States now have 21 months, until 17 October 2024, to transpose its measures into national law. The expanded scope of this legislation includes more sectors and services as either essential or important entities including providers of public electronic communications networks or services, digital services, and space. NIS2 covers three main objectives: increase the level of cyber-resilience of a comprehensive set of businesses operating in the European Union, reduce inconsistencies in resilience across the internal market in the sectors already covered by the directive, and improve the level of joint situational awareness and the collective capability to prepare and respond.


- Each individual country within the EU is responsible for how it might implement Directives. They also have latitude to implement its own additional rules. Examples of national guidelines include:

 **France** - In August 2021, France's Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) published a guide about the **security recommendations for a system of connected objects**. It can be used to design such a system or to facilitate its security analysis. The guide also aims to formulate technical recommendations making it possible to respond to security threats. Its recommendations cover the transportation and storage of data (including confidentiality and integrity), the use of standards and specific protocols, abnormal behaviour monitoring, and authentication, amongst other things.

 **Netherlands** - Following a study by the Dutch Radiocommunications Agency, it issued a set of eight **essential requirements for securing IoT consumer devices**. The requirements included that passwords comply with industry standard digital identity guidelines, network traffic be encrypted, and that vendors must be able to initiate firmware updates.

 **Spain** - In May 2020, the Spanish National Cybersecurity Institute (INCIBE) published its **Security in the installation and use of IoT devices: An approach guide for the entrepreneur** guidelines to help companies safely implement IoT devices in their organisations. The guidelines list multiple recommendations to take into account, to make safe use of IoT devices in the company. These related to passwords, encryption, and updates, amongst other things. Recommendations also include minimising the use of IoT devices, using only those that are strictly necessary, using perimeter security, and implementing regular audits.

 **India** - The Department of Telecommunications (DoT) in India has published a Code of Practice for securing consumer IoT, which includes no universal default passwords, minimising exposed attack surfaces, ensuring software updates, and securing of personal data.

 **Japan** - In September 2017, the Japanese Software Reliability Enhancement Center, Technology Headquarters, Information technology Promotion Agency (IPA/SEC) compiled the **Safety/Security Development Guidelines** to be at least considered by companies involved in devices and systems in a the "Smart-society". This included avoiding default passwords, requiring automatic and/or manual updates, tracking IoT risks after market release, and verifying the design of devices and systems. In August 2022, the Japanese Ministry of Internal Affairs and Communications Cyber Security Task Force published, **ICT Cyber Security Comprehensive Measures 2022**. The cybersecurity guidelines were published to address issues related to cybersecurity in response to trends such as the increasing complexity and sophistication of cyberattacks and expanding vulnerabilities. The measures included a requirement to proactively warn users of IoT devices of cybersecurity issues, promote secure IoT device settings, and prioritise secure-by-design approaches.



Mexico – In December 2022, Mexico's Instituto Federal de Telecomunicaciones (IFT) published a document, **Code of Best Practices for the Cybersecurity of Devices of the Internet of Things**, providing recommendations and best practices including unique passwords, authentication mechanisms, vulnerability management, software updates, restricted use of IoT devices that cannot update their own software, and protection of personal data.



South Korea – An **IoT security certification system** has been introduced to issue a certificate by testing whether IoT products are suitable for information protection certification standards. The certification is provided by Korea Internet & Security Agency (KISA) with Korea Testing & Research Institute (KTC) and Korea Information and Communication Technology Association (TTA) acting as its test agencies. The certification includes three grades: Lite, Basic, and Standard. Testing and certification criteria cover secure authentication, data protection passwords, software security, updates and technical support, operating system and network security, and hardware security.



UK – In October 2018, in the United Kingdom, the Department for Digital, Culture, Media and Sport (DCMS), in conjunction with the National Cyber Security Centre (NCSC) published the **Code of Practice for Consumer IoT Security** which laid out some practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services. Implementing its thirteen guidelines will contribute to protecting consumers' privacy and safety and make it easier for them to use their products securely. It will also mitigate the threat of Distributed Denial of Service (DDoS) attacks that are launched from poorly secured IoT devices and services. Provisions of the Code of Practice include: no default passwords, implementation of a vulnerability disclosure policy, software updates, secure communications, minimisation of exposed attack surfaces, verification of software integrity, personal data protection, resilience to outages, and easy installation and maintenance of devices. The stricter **Product Security and Telecommunications Infrastructure Act 2022** came into force in April 2024 to make provisions for the security of internet-connectable products and communications infrastructure. This law gives the relevant UK minister the power to specify requirements ("security requirements") to protect or enhance the security of relevant connectable products made available to consumers in the United Kingdom and users of such products. These regulations will be applicable to manufacturers, importers, and distributors of interconnected products in the UK. The regulations today specify requirements for passwords, minimum security updates, and statements of compliance.



US – Enacted by the US Government as an Act "To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes", **The IoT Cybersecurity Improvement Act, 2020** is focused on federal procurement of IoT but not private sector or consumers; although the aspiration is that federal procurement volumes will trigger changing behaviour by manufacturers more generally. The Act requires the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) to take specified steps to increase cybersecurity for Internet of Things (IoT) devices. It gives the National Institute of Standards and Technology (NIST) oversight of IoT cybersecurity risks, requiring it to set up guidelines and standards, including over reporting on security issues, and minimum security standards. NIST has a set of voluntary guidelines for manufacturers, which are promoted as capabilities consumers should look for, including a unique identifier and the ability to configure and update firmware. The **NIST Cybersecurity Framework (CSF) 2.0**, released in early 2024, represents a revision on the original NIST framework. It now includes tailored guidance for various industries and introduces a new 'govern' component. This addition underscores the importance of enterprise risk management and the implementation of robust cyber risk strategies. Notably, a significant emphasis is placed on supply

chain risk management, necessitating enhanced scrutiny of suppliers, particularly regarding cybersecurity vulnerabilities. In September 2022, the National Institute of Standards and Technology (NIST) in the USA published **NISTIR 8425 Profile of the IoT Core Baseline for Consumer IoT Products** outlining the consumer profile of NIST's IoT core baseline (the core baseline is a starting point for manufacturers to use in identifying the cybersecurity capabilities their customers may expect from the IoT devices they create) and identifies cybersecurity capabilities commonly needed for the consumer IoT sector (i.e., IoT products for home or personal use). It can also be a starting point for small businesses to consider when purchasing IoT products. The document defines the cybersecurity capabilities expected of IoT products and IoT product developers as a part of a consumer profile. In January 2023, the US introduced the **Informing Consumers about Smart Devices Act**. The act states that each manufacturer of a covered device shall disclose, clearly and conspicuously and prior to purchase, whether the covered device manufactured by the manufacturer contains a camera or microphone as a component of the covered device. The term "covered device" refers to a consumer product that is capable of connecting to the internet, a component of which is a camera or microphone; and does not include either a telephone (including a mobile phone), a laptop, a tablet, or any device that a consumer would reasonably expect to have a microphone or camera or is any device that is specifically marketed as a camera, telecommunications device, or microphone. In July 2023, the Biden-Harris Administration announced **Cybersecurity Labeling Program for Smart Devices to Protect American Consumers** to help Americans more easily choose smart devices that are safer and less vulnerable to cyberattacks. Under the proposed new program, consumers would see a newly created "U.S. Cyber Trust Mark" in the form of a distinct shield logo applied to products that meet the established cybersecurity criteria.

For full details, see the [Transforma Insights Regulatory Database](#) where the specifics of each set of regulations are presented.





06

Data sovereignty and access/portability

Data sovereignty and access/ portability

Many countries have particular rules about the circumstances in which data may or may not be accessed by government, shared within countries and sent overseas. Many of these are relevant to IoT deployments.



China - The **Cybersecurity Law** mandates that personal information and important data collected by critical information infrastructure operators must be stored within China's territory. The National Intelligence Law (2017) Article 7 includes a requirement for all companies registered in China to hand over information to the Ministry of State Security or similar agencies. Article 10 applies the law to technology companies operating overseas. The

Personal Information Protection Law came into force in November 2021. The law states that personal information processed by state agencies shall be stored within the territory of the People's Republic of China; if it is truly necessary to provide it overseas, a security assessment shall be conducted. Security assessments may require support and assistance from relevant departments.}





EU – The EU has a plethora of regulations relating to data use, under the broad umbrella of its data strategy¹. The first major deliverable was the **Data Governance Act** it came into force in June 2022, and became applicable from September 2023. The aim of the act is to reduce the costs of acquiring, integrating and processing data, with the aim of helping enterprises develop new products and services. It provides the processes and architectures for sharing data between enterprise, consumer and government. It specifies who can generate value from data and with what conditions, and removes barriers to data access. The aim is to increase trust in data sharing. The **Digital Markets Act** requires some providers of platform services to be categorised as ‘gatekeepers’ with a requirement to provide data portability.

Within the EDA there are quite onerous requirements on gatekeepers in terms of what services they can provide. On the 6th September 2023 the European Commission stated that it had designated six gatekeepers under the Digital Markets Act: Alphabet, Amazon, Apple, ByteDance (owner of TikTok), Meta and Microsoft. The **‘Regulation on harmonised rules on fair access to and use of data’ (EU Data Act)** is aimed at overcoming what the EU sees as a series of barriers to the greater sharing of data generated by enterprise and consumer IoT devices. It establishes a common framework for establishing what IoT data can be shared and under what circumstances, as well as some obligations and restrictions. In so doing it aims to improve the sharing of data to create a secondary market for services based on IoT data. It also incorporates a number of

¹ See ‘The European Data Act will have huge implications for how IoT services are delivered in the EU and beyond’ (October, 2023) for more on the EU data strategy and the EU Data Act specifically.

subsidiary topics aimed at supporting that core aim.



US - The Clarifying Lawful Overseas Use of Data Act (2018) requires US companies to provide to US government agencies, when requested by warrant, any stored data held on any server, whether in the US or not. Also provided for creation of bilateral agreements. There is some controversy related to this law is it grants extra-territorial rights to US law enforcement agencies. As such it potentially directly conflicts with some of the EU regulations noted above.

Additionally, many countries, including Argentina, Brazil, Indonesia, Nigeria, Turkey and Vietnam have rules requiring that personal data be managed within the country.





07

National resilience

National resilience

As a further evolution on the requirements for device security and data sovereignty, an increasing number of countries are implementing stricter rules related to national resilience and protection of critical national infrastructure (CNI). The NIS2 Directive in the EU, for instance, is being enhanced in some places, notably Sweden and other Nordic countries, as a tougher requirement for CNI and the networks that support them to be able to operate in a closed border situation. Another example is Australia's **Security of Critical Infrastructure (SOCI) Act**. These types of measures have implications for how IoT solutions and the underlying technology (including networks, Connectivity Management Platforms, and application hosting) might be architected.

Elsewhere there are some explicit and implicit prohibition on the use of certain vendors or categories of vendors. In the UK, the new Procurement Act consolidates public procurement into a single set of regulations spanning government, utilities, defence contracts and other critical national infrastructure. It establishes a debarment list which would be monitored by the National Security Unit for Procurement (NSUP) as of October 2024, and reviewed by a minister regularly.

All of this points to a greater polarisation of the IoT regulatory environment, with the need for greater consideration about vendor selection and ensuring that IoT deployments are architected in a way that will be compliant. It does not represent an insurmountable barrier to adoption, but it does require more careful attention.

In the UK, the new Procurement Act consolidates public procurement into a single set of regulations spanning government, utilities, defence contracts and other critical national infrastructure.



08

Regulations in vertical sectors

Regulations in vertical sectors

As well as the general regulations related to IoT and associated fields outlined in the previous sub-sections, there are also numerous vertical-specific regulation which can also be relevant for IoT. In this section we discuss several of the sectors.

8.1

Consumer electronics.

Consumer electronics devices are often subject to extensive regulations relating to product safety, energy efficiency, privacy and security as discussed in the sections above. Most of the rules and regulations on those topics are predominantly targeted at consumer devices or developed with such devices in mind. As such they comprise the majority of the relevant regulation in this space.

8.2

Automotive.

The automotive industry is subject to regulations such as the Federal Motor Vehicle Safety Standards (FMVSS) in the United States which sets safety and performance standards for vehicles which might include IoT-enabled vehicle systems and components. There are also a number of regulations related to IoT-specific use cases outlined below. Emergency call (eCall) deployment has been largely propelled by regulatory compliance. In April 2018, the European Union made eCall service mandatory across 28 countries in Europe. Similar legislation has also been introduced across Japan, the UAE, and Russia. However, countries such as India, the US, and China are still awaiting suitable policies to make eCall service mandatory. In Brazil, an eCall mandate was in discussion for a long time but ended up being suspended.

Regulation can also be a big potential stimulus for the adoption of aftermarket devices. One such regulation is coming in Spain that requires all passenger vehicles to have connected roadside assistance beacons to replace emergency triangles from 1 January 2026. The EU General Safety Regulation passed in July 2022 states that buses and trucks in the EU will have to be equipped with a series of new safety features such as detection and warnings to prevent collisions with pedestrians or cyclists and tyre pressure monitoring systems.

We should note that the use of telematics devices has caused customers to become concerned about their privacy, and how they are allowed to use the vehicles they rent. In some cases, regulations exist to prevent this from happening. For example, New York and California both prohibit the use of telematics devices to levy penalty charges on their customers. Similar limitations, related to privacy, are also restricting the use of dash cams. For example, in Switzerland, the use of dash cams is discouraged in public spaces as it may go against data protection principles; Austria, Belgium, Luxembourg, Portugal and Switzerland have strict laws in relation to the use of dash cams.

Finally, there is a very substantial amount of regulation relating to the use of autonomous vehicles. In September 2022 the European Commission adopted a series of technical rules to ensure that autonomous vehicles such as buses and trucks are safe and their technology is mature enough before they are adopted. Many other countries, including China, Japan and the US, have adopted regulatory frameworks.

8.3



Financial services.

In addition to rules related to personal data privacy as outlined in previous sections, the most relevant requirement for compliance in financial services IoT relates to payment terminals. Here, the global Payment Card Industry Security Standards Council's Data Security Standard (PCI DSS) is the key standard, which is mandated by payment card brands.

8.4



Utilities.

Many smart meter deployments are driven by regulatory requirements. This is particularly true of smart electricity metering. In the EU, the adoption of smart meters was initially driven by the roll-out target of 80% market penetration for smart electricity meters by 2020, established by the EU with the 2009 Third Energy Package plan, although not all member

states have hit the target. In India, the Ministry of Power has stipulated that all industrial and commercial consumers are to have smart meter deployments by 2023 and residential customers by 2025. Provision of smart gas and water metering tend to be more based on commercial models rather than regulation but some particular rules govern the nature of such deployments. For instance, the Chinese government, has mandated the use of locally manufactured smart gas meters.

Many regulations have also been introduced to modernise electricity grid infrastructure. In the US, the Energy Independence and Security Act (EISA) created a national policy to upgrade the national electricity transmission and distribution network. The North American Electric Reliability Corporation (NERC) sets standards related to the grid. In the EU, the "Third European Energy Liberalisation Package" and "Smart Grid European Technology Platform" are focused on the modernisation of distribution networks and the use of localised products for building smart power grids in EU member states. Other governments around the world have introduced programmes for grid upgrades, and in some cases for gas distribution networks.



8.5



Healthcare.

Many countries also maintain regulations specific to healthcare. The most prominent is the US regulation introduced by the Health Insurance Portability and Accountability Act (HIPAA) which governs the privacy and security of protected health information (PHI) collected and transmitted by IoT devices in healthcare settings. It imposes strict standards for data protection, access control, and breach notification. Other countries have similar regulations including Ontario's Personal Health Information Protection Act (PHIPA).

In the EU the Medical Devices Regulation, which came into force in 2021 provides a regulatory framework for devices, components and materials used in a healthcare context.

8.6



Drones.

The use of unmanned aerial vehicles (UAVs) is strictly controlled in almost every country, typically

by rules laid out by the aviation authorities such as the US Federal Aviation Authority (FAA) or the UK Civil Aviation Authority (CAA). Rules govern registration, pilot certification, operational limitation and airspace restriction. These rules will often vary depending on the size and/or weight of the drone.

8.7



Supply chain.

There has recently been an increasing regulatory push for the monitoring of goods, particularly in the pharmaceutical and food industry, whilst in transit. The US FDA's Food Safety Modernization Act (FSMA) and the Drug Supply Chain Security Act (DSCSA) are examples. Enforced since 2017, the FSMA ensures the safety of refrigerated foods in transit, particularly those that present a risk of food poisoning. Similarly, the DSCSA mandates unit-level traceability of the entire pharmaceutical supply chain by 2023.

The United Nations Economic Commission for Europe has published norms on the transportation of perishable foodstuffs and the EU has established Good Distribution Practice (GDP) for the safe transportation of pharmaceutical goods to keep the



product quality intact. The GDP ensures medicines should be stored and transported at the adequate temperature.

In another related field, many countries have set regulations for Hours of Service (HOS) for commercial drivers. The United States Federal Motor Carrier Safety Administration (FMCSA) announced an Electronic Logging Devices (ELD) mandate in 2017 to be implemented in phases. Canada also imposed ELD regulations in 2021. In Canada, the vast majority of for-hire trucks are already equipped with fleet management systems with ELD provision.

8.8



Lone worker safety.

Governments around the world are looking to enhance lone workers' safety by introducing regulations for employees to provide safe workplaces. In the US companies need to provide a safe working environment for workers to comply

with regulations such as the Occupational Safety and Health Act, which mandates safe and hazard-free working environments for all employees. In Alberta, Canada, the Occupational Health and Safety Code 2009, requires employers to provide lone workers with a communication system comprising radio communication, landline or cellular, or any other form of electronic communication to connect them with supervisors or employers. The German Occupational Safety and Health Act and the German Social Accident Insurance Institutions' DGUV Regulation stipulate that employers must ensure the safety and health of their employees by undertaking and providing certain technical safety measures for lone workers².

8.9



Environment.

In the US, the Environmental Protection Agency (EPA) prepares and publishes guidance for air monitoring networks requirements in the Code of

² See 'Worker Safety: 18.2 million connected devices, generating USD3 billion revenue by 2032' (December, 2023)

Federal Regulations. The government issued the Clean Air Act, which states the need for the single-point monitoring for individual facility permits and ambient monitoring to measure the local air quality as per the National Ambient Air Quality Standards. The Clean Water Act, has helped the country to lower the emissions of PM2.5 and PM10, SO2, NOx, VOCs, CO and Pb pollutants³.

8.91



Smart buildings.

Many governments have come up with regulations to improve energy efficiency and air quality in buildings which indirectly promotes the market for smart HVAC products. For example in Spain, the Regulation of Thermal Installations in Buildings (RITE) obliges buildings for administrative or commercial use of more than 1,000 square meters to inform about the energy consumption of the building and the origin of it. It also introduces digitalisation in non-residential buildings with large consumption (such as hotels or shopping centres) whose air conditioning consumption is greater than 290 kW, to take the first step to become smart buildings.

More widely in the EU, two directives are particularly relevant. The Energy Performance of Building Directive (EPBD) advises tools such as building renovation passports and Energy Performance Certificates (EPCs), that contain information related to self-produced or nearby-produced renewable energy. This information requirement would encourage the uptake of smart buildings. The Renewable Energy Directive (RED) requires phasing out inefficient heating systems while guiding

building owners towards renewable choices, which will increase the market for smart and low-carbon technologies.

Other regulations drive the adoption of particular use cases, for instance stringent fire and safety regulations drive the adoption of connected fire alarms. For example, all houses in Scotland are required to have interlinked fire alarms by February 2022. Similarly, the Queensland (Australia) government has made interconnected photoelectric smoke alarms mandatory.

³ See 'Environment Monitoring: 80.5 million connected devices by 2032, generating USD677 million revenue' (February, 2023)



09

Conclusions and recommendations

Conclusions and recommendations

Transforma Insights has identified regulation as the single most significant of its dozen **‘IoT Transition Topics’** (i.e. trends that will have the most impact in the IoT space) for 2024. While some regulations, for instance relating to device certification or product safety standards, have always been part of the fabric of IoT product and solution development, many are becoming dramatically more significant. Particularly we note requirements related to security, procurement and national resilience have become increasingly strict, reflecting the growing importance of IoT particularly for connecting critical national infrastructure. Regulations relating to the management of data, such as the new EU Data Act, have also become much more significant and will demand consideration from any organisation deploying IoT.

Transforma Insights makes the following conclusions and recommendations:

- The regulatory burden is increasing. In future we see a greater level of clarity around the regulations that apply to IoT, which will in most cases be much stricter. Some of today’s approaches for, for instance, multi-country support and associated architectures, as well as data management, used may not work in future.
- Enterprises should conduct a rigorous assessment of the regulations that apply to their IoT deployment. We should note that this report is provided for the purposes of guidance on some of the regulations that may apply to IoT deployments. In all cases, organisations deploying IoT should take legal advice to ensure compliance with the specific relevant regulations.
- Compliance-as-a-service is required. It is no longer enough for vendors in the IoT space to simply ensure that their own offering is compliant (although clearly that is critical). The growing complexity of overlapping regulations means that enterprise adopters will increasingly need help in navigating their way through. For this reason there is a requirement for what we term ‘compliance-as-a-service’, including support on ensuring compliance as well as documentation and auditability of compliance. We also think that this provides an additional revenue source for various vendors in IoT.
- Prepare for a polarisation of global markets. We see the global regulatory environment becoming much more polarised, with a greater politicisation of the supply chain and rules affecting vendor selection, data

sovereignty, national licensing and so on affecting almost every IoT deployment. Vendors need to ensure that the way they architect their operations is appropriate to delivering services in the countries and regions that they address.

- Know your suppliers and components. It is increasingly incumbent on anyone developing an IoT solution to track the Bill of Materials (BOM), and increasingly the Software Bill of Materials (SBOM), of the solution to ensure (and be able to prove with auditability and traceability) compliance.

GSMA Head Office

1 Angel Lane

London

EC4R 3AB

United Kingdom

Tel: +44 (0)20 7356 0600

Fax: +44 (0)20 7356 0601

