

Securing the Internet of Things Together

An Indo-German discussion paper on cybersecurity standards, certification, and regulation for IoT devices

Indo-German Working Group on Quality Infrastructure | Knowledge Series 4

Implemented by



Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Global Project Quality Infrastructure
Country Component India
B5/2, 4th Floor, Safdarjung Enclave
New Delhi 110029, India

T +91 11 4949 5353
E qi-india@giz.de
I www.gpqi.org | www.giz.de/en/worldwide/32230.html

Editors:
Philip Grinsted, Khushwant Singh

Design/layout:
Iris Christmann, Wiesbaden

Photo credits/sources:
© Adobe Stock

URL links:
This publication contains links to external websites. Responsibility for the content of the listed external sites always lies with their respective publishers. When the links to these sites were first posted, GIZ checked the third-party content to establish whether it could give rise to civil or criminal liability. However, the constant review of the links to external sites cannot reasonably be expected without concrete indication of a violation of rights. If GIZ itself becomes aware or is notified by a third party that an external site it has provided a link to gives rise to civil or criminal liability, it will remove the link to this site immediately. GIZ expressly dissociates itself from such content.

On behalf of
German Federal Ministry for Economic Affairs and Energy
Berlin, Germany

January 2020, New Delhi, India

Securing the Internet of Things Together

An Indo-German discussion paper on cybersecurity standards, certification, and regulation for IoT devices

Indo-German Working Group on Quality Infrastructure | **Knowledge Series 4**

About this Publication

This publication was funded by the German Federal Ministry for Economic Affairs and Energy as part of its Global Project Quality Infrastructure (GPQI). GPQI engages in political and technical dialogues with partner countries. Its goal is to reduce technical barriers to trade, enhance product safety, and strengthen consumer protection. The dialogues focus on opportunities and challenges related to standardisation, conformity assessment and accreditation, and market surveillance.

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH – the German Agency for International Cooperation – has been commissioned by the German Federal Ministry for Economic Affairs and Energy to support the implementation of GPQI in Brazil, China, India, and Mexico.

The German Federal Ministry for Economic Affairs and Energy and the Indian Ministry for Consumer Affairs, Food & Public Distribution have established the Indo-German Working Group on Quality Infrastructure to strengthen bilateral collaboration. The Working Group brings together representatives from relevant ministries, including the Indian Ministry of Commerce and Industry (MoCI), Ministry of Electronics and Information Technology (MeitY), Ministry of Heavy Industries and Public Enterprises (MoHI), Ministry of Road Transport and Highways (MoRTH), and the Ministry of Power (MoP) as well as from standards bodies (Bureau of Indian Standards, BIS; the German Institute for Standardization, DIN; German Commission for Electrical, Electronic & Information Technologies, DKE), accreditation bodies (Quality Council of India, QCI; Germany's National Accreditation Body, DAkkS), industry associations, companies, technical and scientific institutions.

The agreed cooperation topics reflect key areas of the economic relations between both countries. They include topics ranging from automotive, electric mobility, machinery safety, Industry 4.0, cybersecurity, and data protection to market surveillance. The Indian country component of GPQI supports the implementation of the mutually agreed annual work plan of the Working Group.

At the 6th Annual Meeting of the Indo-German Working Group on Quality Infrastructure on 18 January 2019 in Berlin, both sides agreed to deepen their dialogue on standards and certification for cybersecurity regulation. The scope and covered aspects of this publication were initially discussed during an expert workshop on standards and certification for Internet of Things (IoT) devices with around 30 participants from the government, subordinate organisations, and the private sector on 16 May 2019 in Mumbai.

The publication was prepared in collaboration with the Bureau of Indian Standards (BIS), the Data Security Council of India (DSCI) and with support of Dr Dennis-Kenji Kipker (University of Bremen, Germany, Legal Advisor to DKE) as well as experts from TÜV Rheinland India Pvt. Ltd. Copy-editing was supported by Dr Kari Hiepko-Odermann. It is the fourth volume in a series of publications on quality infrastructure in India and Germany.

The presentation of the material in this publication does not imply the expression of any opinion whatsoever by the German or Indian Government. The publication was produced without formal editing from the German Federal Ministry for Economic Affairs and Energy or any Indian Ministry.

Foreword

Connected devices are becoming parts of our everyday lives – and so does cybersecurity. Much is at stake in the Internet of Things (IoT): the protection of our personal data, our safety when using smart devices, and the functioning of our increasingly digitised industries.

How to best regulate cybersecurity is a question for governments worldwide. I very much appreciate that India and Germany have joined hands to evaluate and address the challenges lying before us together. Aligned regulations ensure a high degree of security and enable mutual learning. It also eases cross-border business as companies do not have to comply to different regulations.

Governments cannot solve the complex issue of cybersecurity of IoT alone. It needs a collaborative effort of the public and private sector. Both bring in their respective strengths: the innovative power of companies to develop state-of-the-art technical solutions – for example in standardisation – and the trusted regulatory oversight and rule-setting of governments.

India and Germany have set up two complementary forums which can address this issue together: The Indo-German Digital Dialogue between the Indian Ministry of Electronics and Information Technology (MeitY), and the German Federal Ministry for Economic Affairs and Energy (BMWi) as well as the Indo-German Working Group on Quality Infrastructure between the Indian Ministry of Consumer Affairs, Food & Public Distribution (Mo-CAF&PD) and the German Federal Ministry for Economic Affairs and Energy (BMWi).

These two forums allow us to not only discuss high-level regulatory aspects, but also their technical implementation. In a fast-changing field like IoT security, the technical implementation of regulations supported by standards and conformity assessment is decisive.

I would like to express my appreciation to the Data Security Council of India (DSCI) and the Bureau of Indian Standards (BIS) for their collaboration in developing this publication, and the various German and Indian stakeholders from industry, standardisation bodies, and further institutions who contributed with their expertise.

This publication is a great reference of our strong relationship and will surely benefit the citizens of both countries.

Mr Stefan Schnorr
Director-General
Digital and Innovation Policy
Federal Ministry for Economic Affairs and Energy
Germany

Foreword

The Internet of Things (IoT) is a network of ‘Things’ that is connected to the internet. In today’s world almost most of us in one way or the other are connected to the internet. Involving billions of intelligent systems and millions of applications, IoT ecosystems drive new consumer and business behaviors which demand increasingly intelligent solutions. In turn, by 2020 this is expected to drive almost 3 trillion US dollars in new business opportunities for the different vendors and companies that capitalize on the IoT ecosystems.

In today’s world of rapid technological growth, IoT is entering our daily lives and spreading the digital layer around people, organizations and many entities. Henceforth, security risks pertaining to IoT are also growing and are evolving rapidly. In addition, the lack of security awareness on the part of users adds to the huge risk of cyber-attacks.

The threats and risks related to the IoT devices, systems and operations are manifold. Hence, it is important to understand what needs to be secured in an IoT ecosystem and to develop specific security measures by way of standards, certification and regulatory frameworks to protect the same from cyber threats.

This discussion paper is an effort to understand the IoT ecosystem and the related security concerns of IoT devices, especially considering regulatory, standardization and certification aspects of India and the EU. This paper will help in understanding the present position of regulations, standards and certification frameworks. It is intended to raise awareness among stakeholders for continued discussions.

I hope all the stakeholders will benefit from it as per their respective requirements.

Mr Pramod Kumar Tiwari
Director General
Bureau of Indian Standards

Foreword

The advent of the 4th industrial revolution is creating an environment in which everything will be interconnected and intelligent. IoT is the foundation for ushering in this new hyper connected society straddling the physical, digital and virtual worlds. Globally IoT has gained centre stage in the innovation agenda of both industry and academia with cutting edge research and applications of converged technologies for Smart 'X' scenarios. IoT integrated with cloud, and its confluence with AR/VR, AI/ML and analytics is driving rapid growth of IoT across various sectors. While globally Industry 4.0 and healthcare has driven the rapid proliferation of IoT, in India we also see the possibility of Agritech emerging as a key domain to harness the benefits of IoT.

As everything becomes interconnected and intelligent, IoT brings huge economic and functional value to drive digital transformation of businesses and government service delivery alike, leading to a better standard of life for citizens and economic benefits to the country. It is estimated that the connected devices would touch 30 billion by 2020 and 50 billion by 2025, and an economic value of 1.46 trillion USD. This brings attention to security, privacy, resiliency and trust of IoT, and imperatives for trustworthy IoT. Authorization and authentication of IoT, IoT metadata, standards, interoperable protocols, and protocols integration and convergence pose several challenges to security, privacy and trust.

The fundamental objective of IoT security is to preserve privacy, confidentiality, ensure the security of the users, infrastructures, data, and devices of the IoT, and guarantee the availability of the services offered by an IoT ecosystem. In this background it has become imperative for business to focus on cybersecurity and privacy standards that are risk based and internationally harmonised, to create sustainable business models to harness the true potential of IoT devices.

Data Security Council of India (DSCI) is delighted to collaborate with Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and contribute to this discussion paper, to facilitate deliberations between the Indo-German Working Group on Quality Infrastructure and strengthen bilateral collaboration.

Ms Rama Vedashree

CEO

Data Security Council of India

Table of Contents

List of Abbreviations	07
Executive Summary	09
Introduction	12
Regulation of IoT Security	16
India	17
Germany	24
European Union	27
International Approaches to IoT Security Regulation	30
Comparison of IoT security regulations in India and EU/Germany	33
Standards for IoT Security	35
International	36
India	38
Europe	39
Germany	39
Certification of IoT Security	40
India	41
European Union	42
Germany	47
International	47
Security of IoT Devices - Discussion Points for the Road Ahead	48
Conclusion	51
References	52

List of Abbreviations

AktG	German Joint-Stock Companies Act
AtG	German Atomic Energy Act
BIS	Bureau of Indian Standards, Government of India
BMI	Federal Ministry of the Interior, Building and Community, Federal Republic of Germany
BMWi	Federal Ministry for Economic Affairs and Energy, Federal Republic of Germany
BSI	Federal Office for Information Security, Federal Republic of Germany
BSIG	Act on the Federal Office for Information Security, Germany
CAB	Conformity Assessment Body
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT-IN	Indian Computer Emergency Response Team
CII	Confederation of Indian Industry
CISA	Cybersecurity and Infrastructure Security Agency of the United States
CSA	European Union Cybersecurity Act
CSIRT	Cyber Security Incidence Response System
CSL	Chinese Cybersecurity Law
DG CNECT	European Union Commission's Directorate General for Communications Networks, Content and Technology
DIN	German Institute for Standardization
DKE	German Commission for Electrical, Electronic & Information Technologies of DIN and VDE
DoT	Department of Telecommunications, Ministry of Communications, Government of India
DSCI	Data Security Council of India
EAL	Evaluation Assurance Level
ECCG	European Cybersecurity Certification Group
EDPB	European Data Protection Board
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EnWG	German Energy Industry Act
ETSI	European Telecommunications Standards Institute
EU	European Union
GCS	General Certification Scheme
GDPR	European Union General Data Protection Regulation
GIZ	German Agency for International Cooperation
GPQI	Global Project Quality Infrastructure
IACS	Industrial automation and Control Systems

ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ILAC	International Laboratory Accreditation Cooperation
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
LITD	Electronics and Information Technology Department of the Bureau of Indian Standards
MeitY	Ministry of Electronics and Information Technology, Government of India
MIC	Ministry of Internal Affairs & Communication, Government of Japan
MoCAF&PD	Ministry of Consumer Affairs, Food & Public Distribution, Government of India
MoCI	Ministry of Commerce and Industry, Government of India
MoHI	Ministry of Heavy Industries and Public Enterprises, Government of India
MoRTH	Ministry of Road Transport and Highways, Government of India
MRA	Mutual Recognition Arrangement
MTCTE	Mandatory Testing and Certification of Telecommunications Equipment
NICT	National Institute of Information and Communications Technology
NIS	European Union Network and Information Security Directive
NIST	National Institute of Standards and Technology, United States Department of Commerce
NLF	New Legislative Framework of the European Union
OT	Operational Technology
PPP	Public Private Partnership
QCI	Quality Council of India
QI	Quality Infrastructure
R&D	Research and Development
SCCG	Stakeholder Cybersecurity Certification Group
SCS	Simplified Certification Scheme
SDoC	Self-Declaration of Conformity
SOG-IS	Senior Officials Group – Information Systems Security
TEC	Telecommunication Engineering Centre of the Department of Telecommunications, Ministry of Communications, Government of India
TKG	German Telecommunications Act

Executive Summary

SECURITY, PRIVACY, SAFETY: THE INTERNET OF THINGS (IOT) BRINGS NEW CHALLENGES

The rapid spread of networked products and devices – or Internet of Things (IoT) devices – puts cybersecurity at the centre of attention across sectors. In Smart Cities, Smart Homes, and Smart Manufacturing, or Industry 4.0, IoT devices need to be protected against intentional perpetrators as well as from unintended use. With IoT becoming more ubiquitous, much is at risk: the confidentiality of personal information, the integrity of data, along with the functioning of services and systems.

The security challenges are not limited to cyber space. When unsecure IoT devices are interfered with, they have potential to cause dangerous functions and pose a safety hazard. If a conventional information technology (IT) device like a laptop is being hacked, it might affect its functionality but rarely physically harms its user. This could be different if the security of a smart oven or children's toy is compromised.

IoT therefore raises new questions concerning the interplay between security, safety, and consumer protection. Consequently, it challenges the systems governing the liabilities and responsibilities of companies – especially manufacturers and operators – consumers, and the government.

.....
IoT raises new questions concerning the interplay between security, safety, and consumer protection.

NEED FOR INTERNATIONALLY ALIGNED REGULATIONS, WITH A STRONG ROLE FOR STANDARDS AND CERTIFICATION

Given these challenges, regulators around the world are looking for solutions to secure IoT devices. It is currently a strategically important moment to align regulatory responses internationally to avoid a fragmentation of cybersecurity legislation. Global value networks and cross-border trade require internationally harmonised approaches to strengthen trust by consumers and their safety.

Given the fast pace of technological developments, laws and regulations can only define general security objectives and obligations such as mandating manufacturers to apply 'reasonable' security practices. What practices are regarded as 'reasonable' needs to be defined in standards and guidelines which can be updated more dynamically than laws. Certification based on international standards can play a key role to increase trust and support manufacturers of IoT devices to show compliance with legal requirements.

India and Germany decided to explore their potential alignment of cybersecurity regulations, and corresponding standards and certification. This discussion paper includes a comparison of regulatory approaches for IoT device security in India, Germany, the European Union (EU), and beyond. Specifically, it elaborates on the role of standardisation and conformity assessment in these regulations. It highlights key considerations for policy-makers in this emerging field and aims to deepen the international discourse on harmonised approaches to securing IoT devices.

SIMILAR IN INDIA, GERMANY, EU: IOT A 'SIDE-PRODUCT' IN CYBERSECURITY AND DATA PROTECTION LAWS

This discussion paper describes key laws and policies for IoT in India, Germany, and the EU. It includes the *Indian Information Technology Act, 2000* and draft *Personal Data Protection Bill, 2018*, the German *IT Security Act*, as well as the EU *Network and Information Security Directive and the EU Cybersecurity Act*. In a comparable way, the legal frameworks tend to include general clauses which cover IoT as a 'side-product' under various aspects, in particular regarding cybersecurity and data protection. Moreover, there are similarities regarding the proposed extra-legal concretisation of legal requirements, such as through reference to international standards for IT or cybersecurity.

KEY DISCUSSION POINTS FOR POLICYMAKERS IN INDIA, GERMANY, AND BEYOND

Based on inputs from stakeholders representing government, sub-ordinate institutions, industry, and standardisation bodies, this discussion paper draws attention to the following points for further deliberations.

.....
 In a fast-changing technological context, mandatory standards risk being outdated, obstructing innovation, and increasing compliance costs for companies.

- **Aligning regulations internationally, or at least compliance procedures**
 Internationally aligned regulations reduce compliance costs for companies and for users. If convergence of regulations is not possible, industry representatives would appreciate a harmonisation at the level of compliance procedures, such as standards. This allows for technical harmonisation even for complying with differing regulatory provisions. It was stressed that regulations ought to be technology-neutral to not impede the development of innovative solutions. In a fast-changing technological context, mandatory standards risk being outdated, obstructing innovation, and increasing compliance costs for companies.
- **Priority to internationally harmonised and voluntary standards**
 Industry representatives highlighted the crucial and enabling role of voluntary and internationally harmonised standards. Industry-driven standards and technical specifications are dynamic ways of implementing state-of-the-art technologies and reaching regulatory targets. Industry representatives highlighted the need to counter fragmentation of standards, for example by early international exchange on national standardisation activities, and by giving priority to international standards development.
- **Using flexible certification, internationally recognised**
 IoT security is a moving target and static certificates or labels risk being outdated or ineffective. Industry experts therefore demand flexible conformity assessment which targets processes and approaches. It was emphasised that third-party certification shall not be too time consuming, leading to a longer time-to-market. Otherwise, it could potentially delay the availability of security relevant updates and impede innovation. It is seen as important that product certification is not only a snapshot at a single point of time but assesses the security of a product over its entire life cycle. If the costs are comparatively high, manufacturers are discouraged to re-certify products. International accreditation shall be used to establish trusted marks and labels and counter fragmentation.
- **Agreeing on risk categories and corresponding conformity assessment needs**
 Stakeholders stressed that the type of conformity assessment and involved institutions need to depend on the risk of IoT devices. Depending on the risk of an IoT device, the appropriate conformity assessment procedure can be chosen. Stakeholders would appreciate an aligned approach to risk categorisation and would appreciate further exchange on this. Moreover, the risk categorisation approach needs to be updated regularly to react to new technological developments and changing threat scenarios.

- **Developing joint approaches to product liability issues**

An important question relates to the liability of manufacturers, distributors, conformity assessment bodies, and consumers in case of incidents with a certified product. Stakeholders pointed to the fact that certification alone does not exonerate manufacturers from their responsibilities. The specific liabilities, however, need to be defined – especially with the blurring lines between product safety and security. Given the crucial role of secure and regularly updated software for a device’s functioning, stakeholders suggest that software be regulated as a product rather than a service. Furthermore, liability questions relate to responsibilities for informing users of IoT devices about known vulnerabilities and disclosing security breaches.

This discussion paper concludes by outlining aspects which could be taken up by the Indo-German Working Group on Quality Infrastructure. For example, conducting regular exchanges on the development and review of guidelines and standards that represent reasonable security practices for IoT security which supports both countries’ industries in fulfilling their legal obligations and following state-of-the-art approaches. It is suggested to strengthen the dialogue on risk categorisation approaches and exchange on conformity assessment schemes for the respective risk profiles. Furthermore, the paper proposes India and Germany to strengthen their bilateral exchange on national standardisation activities and intensify their cooperation at the international level. This would support harmonised international standards development and closing of current gaps regarding IoT device security.

INTRODUCTION



Introduction

The internet has led to immense increases in productivity and changed the way people and companies communicate on a large scale. The Internet of Things (IoT) promises to extend these transformations by adding objects which were previously not connected through the internet. Concepts like Smart Cities, Smart Home, and Smart Manufacturing, or Industry 4.0, draw attention to the multiple applications of IoT. Expected benefits include greater efficiency, flexibility, quality, and speed.

A growing concern for all IoT applications is their cybersecurity. How can hacking into a smart speaker be prevented, so private conversations in our homes stay private? How can it be assured that an oven connected to the internet does not pose a fire hazard if its security is compromised? Or, how can a company ensure the security of the ever-increasing number of connected devices controlling production in and outside its plant?

This publication uses the wider terminology of cybersecurity which includes security aspects of information technology (IT), but also security of communication, physical assets, their operation, and national security. The threat to cybersecurity can either come from an intentional perpetrator or from unintended use. Key components of cybersecurity include:¹

- **Confidentiality:** Restricted access to information for authorised people, for example through authentication, encryption, or biometric verification. Privacy can be regarded as one form of confidentiality of personal information;
- **Integrity:** Trustworthiness, correctness, and consistency of information, for example through preventing alteration of data in transit (e.g. distributed ledger technologies, or blockchain);
- **Availability:** Guaranteeing reliable and constant access to information, for example through backup systems and mechanisms to prevent downtime of systems.

IoT poses specific security challenges. A large number of interconnected devices means that many assets are potentially vulnerable – a large surface for cybersecurity attacks and vulnerabilities.² One compromised device may compromise the security of other devices. Large-scale attacks on IoT devices might be less problematic for the individual device but critical overall. If through a cyberattack hundreds of thousands of high-wattage IoT devices – say air conditioners or washing machines – are simultaneously switched on at night, it creates an unexpected spike in energy demand. This may lead to an overload in power grids and potentially to blackouts.

Applied to manufacturing, IoT blurs the traditional lines between operational technology (OT) and information technology (IT). Industrial automation and control systems (IACS) cede being separate and are vulnerable to outside attacks. As OT design usually did not anticipate this threat, the legacy of old hardware makes upgrades difficult.

¹ Compare ISO/IEC 27001.

² European Union Agency for Cybersecurity (ENISA). 2018. *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, p. 16.

IoT raises new questions concerning the interplay between security, safety, and consumer protection.

With IoT, security challenges are not limited to the cyber space. When unsecure IoT devices are interfered with they may cause dangerous functions and posing a safety hazard. If a conventional IT device like a laptop is being hacked, it might affect its functionality but rarely physically harms its user. This could be different if the security of a smart oven or children’s toy is compromised. IoT therefore raises new questions concerning the interplay between security, safety, and consumer protection. Consequently, it challenges the systems governing the liabilities and responsibilities of companies – especially manufacturers and operators – consumers, and the government.

INFO BOX 1: DEFINITION OF IOT DEVICES

The International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) define IoT as “an infrastructure of interconnected entities, people, systems and information resources together with services which process and react to information from the physical world and from the virtual world.”³

For the purpose of this publication, IoT devices are defined as those that

1. incorporate one or several **transducers** such as sensors which allow them to interact with the physical world,
2. have one or several **network interfaces** such as a WiFi or Ethernet connection, and
3. are **non-conventional information technology (IT) devices** unlike smartphones or laptops.⁴

Following this definition, the paper considers both IoT devices used by consumers and for industrial use.

Examples for IoT devices

- smart energy meters
- internet-connected video surveillance cameras
- automated vacuum cleaners connected through the internet
- connected home alarm systems
- condition monitoring devices (e.g. vibration or temperature of machines)

Not considered as IoT devices: laptops, keyboards, routers, smart phones

Now is a strategically important moment to align regulatory responses internationally to avoid a fragmentation of cybersecurity legislation.

Given these challenges, regulators around the world are looking for solutions to secure IoT devices. Now is a strategically important moment to align regulatory responses internationally to avoid a fragmentation of cybersecurity legislation. Global value networks and cross-border trade require internationally harmonised approaches to strengthen trust by consumers and their safety.

Given the fast pace of technological developments, laws and regulations can only define general security objectives and obligations such as mandating manufacturers to apply ‘reasonable’ security practices. What practices are regarded as ‘reasonable’ needs to be defined in standards and guidelines which can be updated more dynamically than laws.

An effective analysis of IoT device security needs to consider different aspects of quality infrastructure (QI), the system comprising standardisation, conformity assessment and accreditation, metrology, and market surveillance (see info box 2). A well-functioning and internationally harmonised QI increases trust of all market participants in the safety of products and services, and reduces transaction costs. The interplay between regulation, standards, and approaches to prove compliance – or conformity assessment – are especially crucial around IoT device security. Because of this, this publication looks at regulations, standards, and conformity assessment in an integrated manner.

³ International Organization for Standardization (ISO). 2019. *Architecting a Connected Future*. <https://www.iso.org/news/ref2361.html>.

⁴ Compare: National Institute of Standards and Technology (NIST), 2019, p. vii.

INFO BOX 2:

Please find further information on standardisation, technical regulation, and conformity assessment in India in the publication “Overview of India’s Quality Infrastructure”. To download your free PDF copy, please visit www.gpqi.org or scan the QR code with your non-IoT smartphone.



Regulatory approaches for IoT device security in India, Germany, the European Union (EU), and beyond are described and compared in this discussion paper. Specifically, it elaborates on the role of standardisation and conformity assessment in these regulations.

This discussion paper highlights key considerations for policy-makers in this emerging field. The objective of this publication is to deepen the international discourse on harmonised approaches to securing IoT devices. Aligned approaches lead to greater consumer safety, national security, and ease cross-border trade in products and services related to IoT. A growing number of different national regulations risks creating technical barriers to trade. While this paper focuses on the Indo-German or Indo-EU context, the matter of this publication is of global relevance.

This publication starts by describing the relevant regulatory system for IoT device security in India, Germany, the EU and further countries (United States, Japan, and China). To initiate the Indo-German dialogue on possible regulatory harmonisation, the publication compares the regulatory frameworks in Germany and India. The subsequent chapters elaborate on existing standards and conformity assessment schemes related to IoT device security in India, Germany, and the EU. This is followed by an overview of key themes around the regulation of IoT device security and perspectives on the role of standardisation and conformity assessment. These perspectives are based on stakeholder inputs from the Indian and German industry and are meant to initiate and frame further discussions. Lastly, the conclusion reflects on the status quo and draws attention to next steps for the Indo-German cooperation.

.....
Aligned approaches lead to greater consumer safety, national security, and ease cross-border trade in products and services related to IoT.



REGULATION OF IOT SECURITY

Regulation of IoT Security

India

The policy and regulatory framework for IoT security in India is spread across different legislations and policies. Key institutions are the Indian Ministry of Electronics and IT (MeitY), the Department of Telecommunications (DoT) of the Indian Ministry of Communications, and the National Institution for Transforming India (NITI Aayog) – the policy think tank of the government of India.

In 2015, MeitY released a draft *Internet of Things Policy* which defined IoT as “a seamless connected network system of embedded objects/ devices, with identifiers, in which communication without any human intervention is possible using standard and interoperable communication protocols”.⁵ The policy remained at a draft stage and is described below.

The following sections give an overview of important acts and regulations with relevance to IoT device security in India.

INFORMATION TECHNOLOGY ACT, 2000

The *Information Technology Act, 2000* (IT Act, 2000) is the special legislation dealing with cyber contraventions, cybercrime, and e-commerce in India. The law covers a variety of subjects associated with regulation of cyber space in India. From the context of IoT the following aspects are essential.

Privacy and Data Protection

The act covers the protection of sensitive personal data or information with further specifications elaborated upon in the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*.

According to section 43A of the act, a body corporate not implementing and maintaining reasonable security practices and procedures in respect of sensitive personal data or information possessed, dealt or handled by it in a computer resource owned, controlled or operated by it, is liable to pay damages to the person so affected for wrongful loss or gain to any person.⁶ The rules mandate the basic principle of privacy law that the body corporate needs to obtain informed consent along with certain privacy compliance practices.⁷

The act, however, does not encompass protection of personal information, in all situations, when used or shared in the context of IoT. Moreover, the act is limited to the use of *sensitive* personal data or information. This includes personal information relating to passwords, finances, health, sexual orientation, medical records and history, and biometric information. According to the act, any information that is freely available or accessible in the public domain or provided under acts such as the *Right to Information Act, 2005* is not regarded as sensitive personal data or information.⁸

Further, Section 72A of the IT Act, 2000, enunciates penalty for breach of the confidentiality and privacy of personal information collected.⁹

⁵ Ministry of Electronics & Information Technology (MeitY). *Draft Policy on Internet of Things*. 2016.

⁶ MeitY. 2000. *Information Technology Act, Section 43A*.

⁷ Ministry of Communications and Information Technology. 2011. *Reasonable Security Practices and Procedures and Sensitive Personal Data or Information. Rule 5*.

⁸ *Ibid.*, Rule 3.

⁹ MeitY. 2000. *Information Technology Act, Section 72A*.

Reasonable security practices and procedures

Under the IT Act, 2000 and the corresponding rules issued in 2011, a body corporate must implement such security practices and standards as well as have a comprehensive documented information security programme and policies that are adequate with the information assets being protected with the nature of business.¹⁰ The security control measures shall contain managerial, technical, operational and physical aspects. The rules identify the international standard ISO/IEC 27001 on “Information Technology – Security Techniques – Information Security Management System – Requirements” as one such standard.¹¹

If a self-regulating organisation chooses security practices different from those formulated in Indian or international standards they need to be audited by an independent auditor, duly approved by the Central Government. This audit shall be carried out at least once a year or as and when the body corporate or a person on its behalf undertake significant upgrades of its process and computer resource.¹²

Unauthorised Access

The IT Act, 2000 also imposes penalties and imprisonment terms up to two years or fine up to 100,000 Indian rupees (approx. 1,300 EUR) or both, on any person who secures access to any electronic record, information etc., and who, without consent of the person concerned, discloses such record, information etc., to any other person.¹³

Damage to computer, computer system etc.

The IT Act, 2000 also covers a variety of actions used to cause damage to computers,¹⁴ computer systems,¹⁵ computer resources¹⁶ or computer networks¹⁷ – these terms cover IoT devices as well. The actions according to Section 43 are as below:

1. Downloading, copying, or extracting any data, computer data base or information from such computers, computer systems or computer networks including information or data held or stored in any removable storage medium.
2. Introducing or causing to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
3. Damage or cause to be damaged any computer, computer system or computer network, data, computer data base or any other programmes on such computer, computer system or computer network.
4. Disrupt or causes disruption of any computer, computer system or computer network.

¹⁰ Ministry of Communications and Information Technology. 2011. *Reasonable Security Practices and Procedures and Sensitive Personal Data or Information*. Rule 8(1).

¹¹ *Ibid.*, Rule 8 (2).

¹² *Ibid.*, Rule 8(4).

¹³ MeitY. 2000. *Information Technology Act, Section 43(a)*.

¹⁴ ‘Computer’ means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network (*Ibid.*, Section 2(1)(i)).

¹⁵ ‘Computer system’ means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions (*Ibid.*, Section 2(1)(l)).

¹⁶ ‘Computer resource’ means computer, computer system, computer network, data, computer data base or software (*Ibid.*, Section 2(1)(k)).

¹⁷ ‘Computer network’ means the inter-connection of one or more computers or computer systems or communication device through– (i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained (*Ibid.*, Section 2(1)(j)).

5. Deny or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means.
6. Provide any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this act, rules or regulations made thereunder.
7. Charge the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.
8. Destroy, delete, or alter any information on a computer resource or diminishes its value or utility or affects it injuriously by any means.
9. Steal, conceal, destroys, or alters or causes any person to steal, conceal, destroy, or alter any computer source code used for a computer resource with an intention to cause damage.

Enforcement Mechanism

Section 43 is an important provision as it identifies different actions causing damage to computers, computer systems or computer networks. The contravener is liable to pay damages by way of compensation to the person affected. It is for the affected person to assess the value of damage caused and approach the appropriate forum for redressal – whether the adjudication officer or a civil court. The pecuniary jurisdiction of the adjudicating officer under the act is up to 50 Mio. Indian Rupees (approx. 640,000 EUR) and if any affected person assesses the value of damage beyond 50 Mio. Indian Rupees, the said person may approach the competent civil court for redressal. A decision or order passed by the adjudicating officer can be appealed to the cyber appellate tribunal.

DRAFT IOT POLICY 2015

This draft policy was created with the intention of developing a connected, secure and smart IoT based system for India's economy, society, environment, and global needs. It remained a draft and has not been accepted as official government policy. Therefore, the following sections are only indicative.

The draft policy proposed that the policy framework of the IoT policy should be implemented via a multi-pillar approach, comprising demonstration centres, capacity building and incubation, research and development (R&D) and innovation, incentives and engagements, human resource development, and standards and governance structure.

Governance Structure

The draft policy proposed to set up a legal framework for issues arising from IoT related products, systems, and services.¹⁸ Guidance was planned to be given by a high-level advisory committee comprising representatives from government, industry, and academia.¹⁹ Additionally, governance committees for different application domains were suggested to be established. These were intended to be chaired by the secretary of respective ministries or departments and to comprise representatives from government, industry, and academia to govern all IoT initiatives, projects, and assess their progress against planned timelines.²⁰ Lastly, the policy suggested the creation of a programme management unit. The unit was meant to give ongoing support in operationalising the IoT Policy, implement initiatives, carry out performance-reviews, and make suggestions to the advisory and governance committees.²¹

¹⁸ MeitY. 2015. *Draft Policy on Internet of Things*, p. 16.

¹⁹ *Ibid.*

²⁰ *Ibid.*

²¹ *Ibid.*, p. 16-17.

Standards

The draft policy proposed to appoint relevant coordinating organizations to drive and formalise 'globally acceptable standards' relating to technology, process, interoperability and services, with a special focus on the following areas:²²

- IoT standardisation
- Spectrum energy communication protocols standards
- Standards for communication within and outside the cloud
- International quality/integrity standards for data creation, data traceability
- Standards for energy consumption
- Device security and safety standards
- Data privacy, data accuracy and integrity, and security standards.

It also proposed to create a national expert committee for developing and adopting globally established and interoperable IoT standards in the country. The expert committee should include industry experts and organizations in areas such as:²³

- Identification Technology – development of open framework for IoT;
- Architecture Technology – IoT architecture, platform interoperability;
- Communication Technology – ultra-low power chipsets, on-chip antennas, ultra-low power single chip radios, ultra-low power system on chip;
- Network Technology – self-aware and self-organizing networks, storage and power networks, hybrid networking technologies;
- Software and algorithms – next generation IoT based social software, enterprise applications;
- Hardware – multi-protocol/-standard readers, sensors, actuators etc.;
- Data and signal processing technology;
- Power and energy storage technologies (energy harvesting and conversion, long range wireless power);
- Security and privacy technologies;
- Material Technology (silicon, semiconductor manufacturing etc.);
- Participation in standards committees of International Telecommunication Union (ITU), Institute of Electrical and Electronics Engineers (IEEE), and other relevant global forums for standards making in IoT;
- Certification laboratories.

²² *Ibid.*, p. 11.

²³ *Ibid.*, p. 11-12.

NATIONAL CYBER SECURITY POLICY, 2013

MeitY released a *National Cyber Security Policy* in July 2013 with the goal to guide actions related to cybersecurity and enable organisation in designing cyber security policies. The policy gives insights into measures required to protect information, information systems and networks, and the government's approach to cyber security in India.

The policy describes the need to create an assurance framework for the design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology and people).²⁴ For this, it names examples such as certification of information security management systems (ISMS) according to ISO/IEC 27001, penetration testing, vulnerability assessments, applications security testing, and web security testing. The establishment of a testing infrastructure for IT security products and compliance verification according to global standards and practices is also one measure described to reduce supply chain risks.

The policy describes the goal to develop a dynamic legal framework and its regular review to address challenges due to new technological developments. It described the aspiration for this legal framework to be harmonised with international ones.

Given the dynamic technological developments in cyber security and cyber risks, the policy recommends developing public private partnership (PPP) models to strengthen the collaboration and engagement with relevant stakeholders regarding cyber threats, vulnerability, breaches, protective measures, and the adoption of best practices.

Concerning critical information infrastructure, the policy encourages the development of plans for their protection, including guidelines and standards. It also promotes the use of validated and certified IT products, possibly by mandating it.

NATIONAL DIGITAL COMMUNICATIONS POLICY 2018

In September 2018, the Department of Telecommunications (DoT) of the Ministry of Communications released the *National Digital Communications Policy, 2018* which updated and replaced the *National Telecom Policy of 2012*. The objective of the policy is to lay out a framework to create a competitive telecom market in India and contribute to strengthening India's long-term competitiveness.

One of the described strategies to attract investments, spur Innovation, and promote manufacturing in emerging technologies is to simplify licensing and regulatory frameworks while at the same time ensuring appropriate security frameworks for IoT and M2M. Such frameworks are meant to incorporate international best practices.²⁵

To meet the goal of ensuring digital sovereignty, safety, and security of digital communications, the policy's proposals include developing security standards for equipment and devices. These shall be met by introducing telecom testing and security certification, aligned with global standards on safety and security. India's participation in global standards development organisations shall be strengthened to ensure that local needs of the Indian communications industry are considered.

²⁴ MeitY. 2013. *National Cyber Security Policy*, p. 5.

²⁵ Department of Telecommunications (DoT). 2018. *National Digital Communications Policy*, p. 13.

Furthermore, it proposes to harmonise the legal and regulatory frameworks applicable to security standards, such as the BIS Act, Indian Telegraph Act, and MeitY's Compulsory Registration Order for electronics and IT products.

The goal of strengthening security testing processes shall be achieved by enhancing institutional capacities to perform testing, setting up domestic testing hubs and laboratories, and establishing comprehensive security certification regimes based on global standards.

The *National Digital Communications Policy* proposes to formulate a policy on encryption and data retention by harmonising India's legal and regulatory regime on cryptography with global standards.

Further, the policy suggested to set up a sectoral Cyber Security Incidence Response System (CSIRT), improve coordination between agencies such as the Indian Computer Emergency Response Team (CERT-IN) and sectoral CERTs, and enforce obligations on service providers to report data breaches.

DRAFT PERSONAL DATA PROTECTION BILL, 2018

MeitY released the *Draft Personal Data Protection Bill, 2018* which brings personal data processing by IoT devices into its purview. The bill lays down certain security safeguards that the processor or controller of such processing activity must implement. These are:²⁶

- a) use of methods such as de-identification and encryption;
- b) steps necessary to protect the integrity of personal data; and
- c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

Section 31 of the draft bill prescribes that every data fiduciary and data processor must undertake a review of its security safeguards periodically and take appropriate measures accordingly. After finalisation of the bill it would still need to be defined what counts as appropriate security safeguards.

²⁶ MeitY. 2018. *Draft Personal Data Protection Bill, Section 31*.

INFO BOX 3:**Technical Report - Recommendations for IoT / M2M Security in India**

In January 2019, a technical report was published giving recommendations for IoT or Machine-to-Machine (M2M) security in India. The report was developed by a working group set up by the Telecommunication Engineering Centre (TEC) of the Department of Telecommunications, Indian Ministry of Communications. It defines that IoT security “deals with safeguarding connected devices, physical and virtual, in addition to the networks and IT security, for the Internet of Things”.²⁷

With the technical report the working group was tasked to prepare recommendations in the following areas:

- Incorporation of minimal security standards for M2M products and services, considering their interoperability;
- Defining security guidelines regarding aspects such as data ownership, sensitive data, location of application services, and location of remote terminal unit;
- Defining policies and standards for security to connect legacy and non-IP devices;
- Defining precautions and security conditions for voice/SMS/MMS/video on M2M;
- Requirements for security certification for M2M products.

The working group states that a crucial question is how to protect data generated by end-point devices and applications. Therefore, it recommends classifying IoT use cases and match mandatory parameters, for example relating the identity of devices, service providers, applications, and servers. Among several recommendations, the report proposes six assurance levels for end-point devices (ranging from ‘no authentication and identification’ to ‘biometric authentication’).

The report makes proposals about the registration of devices, applications, and service providers with DoT and the National Trust Centre – which is proposed to be set up under the umbrella of DoT. Certification shall be based on the classification of use cases and applications and include certification based on essential requirements framed under TEC’s Mandatory Testing & Certification of Telecommunications Equipment (MTCTE; details in Chapter on Certification below) and schemes by independent conformity assessment bodies (CABs).

- ◉ The report can be downloaded on the TEC Website (<http://www.tec.gov.in/technical-reports/>).

²⁷ Telecommunication Engineering Centre (TEC). 2019. *Recommendations for IoT/M2M Security*, p. 25.

Germany

German law does not regulate cybersecurity through codification so that numerous regulations for individual cases can be found in different laws. A distinction must be made between special laws on information security and the general legal requirements of corporate compliance, which may also include cybersecurity issues today due to their wide range of interpretation.

Section 43 of the *German Limited Liability Companies Act* (GmbHG), section 91 paragraph 2 and section 93 paragraph 1 of the *Joint-Stock Companies Act* (AktG) can be mentioned as an example. According to these regulations, the managing directors and the management board each have a duty to provide “diligence obligations” in general and to take measures to ensure that “developments endangering the survival of the company” are recognized at an early stage. In this case, the “care of a proper and conscientious business manager” is required. Today, these general diligence obligations are recognized to include cybersecurity measures, for example a company’s IoT products. This shows that possible legal obligations regarding cybersecurity do not always have to be clear from the wording of law.

IT SECURITY ACT (IT-SIG)

The German IT security law of 2015 is to be seen in this context, because as an Article Act, it has not created a new, independent code on cybersecurity, but amended numerous individual laws in relation to cybersecurity, such as the *Atomic Energy Act* (AtG), the Act on the *Federal Office for Information Security* (BSIG), the *Energy Industry Act* (EnWG) or the *Telecommunications Act* (TKG).

Generally, it can be said that, the first IT-SiG does not contain an explicit reference to IoT device security, but refers primarily to the IT security of Critical Infrastructures and the expansion of the powers of the Federal Office for Information Security (BSI) as the central German state agency for the promotion of cybersecurity.

The comprehensive task catalogue of the BSI is described in section 3 BSIG. Regarding IoT devices, the two main features to be emphasized for the BSI are: section 7 BSIG (Warnings) and section 7a BSIG (Investigation of Security in Information Technology).

BSI is authorised to address warnings to the public or to the interested parties about security vulnerabilities in IT products and services, may warn about malicious programs, or point out data breaches. Furthermore, the BSI may recommend the use of certain security products. In principle, the manufacturers of the affected products should also be included. If there is enough evidence that cybersecurity threats originate from the product itself, the public warning may also name the manufacturer and product.

BSI may also investigate IT products and systems made available or intended to be made available on the market. Third parties may also be used to support the investigation, if the interests of the manufacturer do not conflict with this. In principle, the results obtained from the investigation may also be published. In this case, the manufacturer can comment on this case within a reasonable period.

Looking more closely at the legal changes brought about by the IT-SiG, it is noticeable that many of the laws have a similar wording despite the diversity of their respective fields of application. Thus, phrases such as “reasonable technical and organizational arrangements”, “reliable”, “safe”, “proper” and “state of technology” are frequently found. The terms themselves are not further specified by the law. These “indeterminate legal terms” or “general clauses” are regulatory limits of the law because technological development is so rapid that legislators are unable to describe the technical details in the respective laws. The openness of indefinite legal concepts thus offers the possibility of incorporating technical requirements into the law via sources outside the law. An important source of interpretation are technical norms and standards.

DRAFT IT SECURITY ACT 2.0 (IT-SiG 2.0)

The German Federal Ministry of the Interior, Building and Community (BMI) published a draft version of an updated IT-SiG – the so-called IT-SiG 2.0 – in April 2019. The following sections deal with this draft which, may change significantly in the future.

The IT-SiG 2.0, like the first IT-SiG from 2015, is also an article law, so that in turn various individual laws are amended. Regarding the specific legislation concerned, there are key changes, in particular in the BSIG.

It is characteristic that the IT-SiG 2.0, in implementation of the national cyber security strategy of 2016, particularly aims at consumer protection, making it more relevant to IoT than the 2015 law. While IoT is not explicitly taken up by the regulatory system or in the focus of the law, it is addressed in the recitals of the law. Essentially, two things are referred to here: Not only is the spread of IoT increasing, but the devices are often not developed under adequate security requirements and thus have weak points through networking. Specifically, the following regulatory proposals should be underscored for IT-SiG 2.0 from the IoT point of view:

- **Section 3 paragraph 1 sentence 2 letter d) BSIG (draft):** Extension of the tasks of the BSI to promote consumer protection and consumer information, in particular by providing advice, information and warning of possible consequences of incorrect or inadequate security measures.
- **Section 7b paragraph 1 BSIG (draft):** The BSI can detect malicious programmes, security vulnerabilities and security risks in publicly available IT systems accessible via the Internet, if they are unprotected and therefore endangered.
- **Section 7b paragraph 4 BSIG (draft):** Authorization of the BSI to use active ‘honeypots’ to obtain information on malicious programs and methods of attack.
- **Section 109a paragraph 8 TKG (draft):** Authority to order IT security measures directed at the telecommunication service provider against Ransomware of Things, to combat Bot-nets and to clean up infected data processing systems, because many IoT users are unaware of their device having been compromised with malware.

There are also other regulatory proposals in the IT-SiG 2.0 which, although not explicitly aimed at IoT, can contribute to improving the security of IoT products as well:

- **Section 4b BSIG (draft):** Strengthening the role of the BSI as a central information security body in Germany. The BSI establishes a general reporting centre for cybersecurity, which also accepts information anonymously. Afterwards the authority has the possibility to inform the public, for example, if products or services show security gaps.
- **Section 5d paragraph 1 BSIG (draft):** The BSI may collect stock data (for example contract name, address, and date of birth) of telecommunication service providers to contact affected people due to purposes of IT security. The request for information extends also to IP addresses.
- **Section 7 paragraph 1 BSIG (draft):** The BSI may issue warnings to the public or those affected, highlighting security vulnerabilities in IT products or services, warning against malicious programmes, and providing information on security-related IT properties of products. In addition, the BSI can recommend safety measures and the use of certain products.
- **Section 7a BSIG (draft):** The BSI may investigate IT products made available on the market or intended to be made available on the market for cybersecurity purposes. For this, the BSI can obtain information from the manufacturer. If the manufacturer does not fulfil its obligation to provide information, the BSI can inform the public about this situation.
- **Section 8a paragraph 6 BSIG (draft):** The first IT-SiG from 2015 already contained special regulations for Critical Infrastructures, which shall be extended by IT-SiG 2.0. As far as IoT devices in Critical Infrastructures are core components with a control function, they may only be obtained from manufacturers who have issued a trustworthiness declaration. This extends to the entire supply chain of the manufacturer.
- **Section 8h BSIG (draft):** Manufacturers of IoT products have the responsibility to notify the BSI of significant disruptions in the IT security features of their products immediately if the use of the product can lead to a failure/significant malfunction of critical equipment.
- **Section 9a BSIG (draft):** A central consumer protection regulation, which can also be applied to IoT products, concerns the introduction of a voluntary IT security marking.

European Union

LEGAL SYSTEMATIC AND CORRELATIONS WITH EU DATA PROTECTION LAW

There is currently no special law in EU legislation dealing exclusively with cybersecurity and IoT. In this regard, the legal situation is comparable to the regulatory structure in Germany. Intersections to IoT can result from different EU laws depending on the application scenario, for example:

- Directive 2014/53/EU of 16th April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (RED-Directive);
- Regulation (EU) No 910/2014 of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS-Regulation)

In addition, the overlap of cybersecurity and data protection must be considered, in so far as IoT devices process personal data that must also be protected technically and organizationally against unauthorized access. The following European laws should be mentioned in this connection:

- Regulation (EU) 2016/679 of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR)
- Directive 2002/58/EC of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, ePrivacy Directive)
- Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, ePrivacy Regulation, ePR, currently only as a draft version)

In the context of EU data protection law, especially Article 32 GDPR is of high importance. This provision regulates the security of the processing of personal data. For this purpose, it is determined that the responsible person must take appropriate technical and organizational measures in order to ensure a level of protection appropriate to the risk. This includes, among others, the following aspects:

- Pseudonymization and encryption
- Ensuring the main goals of IT security: Confidentiality, integrity, availability and resilience of processing systems and services
- Ability to restore the availability of personal data after a technical incident
- Regular review and evaluation of data security measures

NETWORK AND INFORMATION SECURITY DIRECTIVE (NIS)

Unless technical or organizational measures to protect personal data have to be taken, the *Network and Information Security Directive 2016/1148* (NIS) sets out one of the main regulation tasks of the new European cyber security law. The directive, which came into force in August 2016, was to be transposed into national law by EU Member States until May 2018.

As the first piece of legislation aimed at promoting European cybersecurity, it focuses primarily on the protection of the digital internal market. The content requirements that are prescribed in this regard - are in many places comparable to the first German IT-SiG. For example, operators of essential services, a European term for Critical Infrastructures, must establish technical and organizational cybersecurity measures. From this, however, no relevance for IoT can be derived. Of greater interest, although again not directly relevant to IoT, are the NIS Directive requirements stipulating that digital service providers, which include online marketplaces, online search engines, and cloud computing services, also have to provide technical-organizational measures for cybersecurity.

CYBERSECURITY ACT (CSA)

The latest European Cybersecurity Legislative Act is the *EU Cybersecurity Act* (CSA), Regulation 2019/881, which entered into force on 27 June 2019. The core elements of the CSA are the introduction of a European cybersecurity certification system and the comprehensive restructuring of ENISA, which will have a permanent mandate.

The CSA explicitly addresses the topic of IoT. It acknowledges the expected immense growth in the number of IoT products in the EU, the rising importance of consumer confidence in such products, and the responsibility of the EU to promote it. The act mentions product categories such as connected and automated cars, electronic medical devices, industrial automation control systems, and smart grids.

An EU-wide certification framework for cybersecurity of (IoT) products should not only ease access to foreign markets for European-wide companies but strengthen the EU Digital Single Market. The certification under the CSA is intended to be voluntary unless otherwise specified in Union or Member State law.

While the CSA enables the creation EU certification schemes it does not introduce operational schemes itself. Certificates will be recognised across all EU member states, thereby easing cross-border trade, and enhancing the understanding of the security features of a product or service. It is expected that the EU Commission will present a list of mandatory certification schemes until 2023.

- Detailed information about the European cybersecurity certification framework can be found in Chapter “Certification for IoT Security”.

The CSA also makes extensive references to standardisation. It says that certification schemes shall be based on European or international standards, unless those standards are ineffective or inappropriate to achieve the cybersecurity objectives. When preparing the EU cybersecurity certification schemes, ENISA is encouraged to regularly consult standardisation organisations. EU cybersecurity certification schemes will replace existing national certification schemes, but existing certificates issued under national cybersecurity certification schemes will remain valid until their expiry date.

Several critical issues of the implementation of the CSA are currently being discussed, including the compatibility of the new certification regimes with the EU's existing New Legislative Framework (NLF), whether EU product legislation shall make reference to the CSA, and the concrete ways that different stakeholders can contribute to the CSA's newly created working and interest groups.

FURTHER DIRECTIVES

In the case of IoT, cyber security is increasingly addressing consumer protection issues directly. In this context, besides the EU NIS Directive and the EU Cybersecurity Act, there are two further directives that must be transposed into national law by the EU Member States by 2021: The Directive on certain aspects concerning contracts for the supply of digital content and the Directive on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC.

Both directives pursue similar objectives; the simplification and unification of the EU's digital internal market and the promotion of EU-wide consumer protection in the digital domain. The scope of application therefore includes digital content, digital services and goods with digital elements. These include in particular IoT products such as intelligent refrigerators, smart watches, cloud services, and streaming services.

It is stipulated for the products concerned that they must be in accordance with the contract. Contractual compliance also includes IT security. For example, an entrepreneur must ensure to a consumer that IT security updates are made available for their products and services in order to ensure compliance with the contract. The guidelines are of a mandatory nature and are associated with comprehensive statutory consumer rights for enforcement purposes, some of which go far beyond existing Member State laws.

International Approaches to IoT Security Regulation

As smart devices are becoming more and more an ordinary part of nearly everyone's daily work and private life, several countries address cybersecurity issues of IoT in their current legislation. Here we look at example of the United States, Japan and China as these are among the countries that have passed regulations of national and international significance. It is noteworthy that these legislations address IoT issues at different levels of granularity, so that the legal situation is comparable to certain approaches in German and EU law.

UNITED STATES

In the US, there is no comprehensive law on regulation of IoT security at the federal level, but several legislative and pre-legislative approaches are currently being taken. With the Considerations for Managing IoT Cybersecurity and Privacy Risks (NISTIR 8228), the US Department of Commerce National Institute of Standards and Technology (NIST) published voluntary protective guidelines for IoT users.

The guidelines define three security goals: 1) The protection of device security, 2) data security, 3) and the individuals' privacy. This shall be achieved by requiring the producers of such devices to ensure that their devices are publicly recognized as an IoT device, so that the user is aware of potential risks. In addition, the devices need to ensure that users can see with which other IoT devices their devices connect and which functions are currently used.

Manufacturers of IoT products are required to not only reduce the security risks of their own device, but also protect users from risks due to correlation with other devices that are normally operated in the context of an IoT product. It is also prescribed that manufacturers must provide user recommendations on how to handle cybersecurity risks which are caused using the IoT product.

With the new *Cybersecurity and Infrastructure Security Agency Act of 2018* (H.R.3359), which amends the *Homeland Security Act of 2002*, the US want to set concrete standards for the country's security in the digital world. The act renames the former "National Protection and Programs Directorate" to "Cybersecurity and Infrastructure Security Agency" (CISA). The CISA can be considered as a general authority which is not only focused on IoT device security, but may consider IoT security as well, when there are links to national interests. The agency is to ensure that the US Government is aware of all current situations in the world of cyber and provides it with cybersecurity tools, incident response services, and assessment capabilities to protect the networks which support the essential operations of federal civilian departments and agencies. CISA coordinates security and resilience efforts, provides security training and plans the work on identifying and addressing the most important risks which could put the nation's critical infrastructures in danger.

Further changes in IoT security regulation in the US might be expected soon. Recently, the nation's mayors approved the improvement of data security and infrastructure in the US at their 2019 annual meeting. Greater protection against the risks of physical intrusion and infiltration of edge sensors associated with the deployment of smart city technologies is demanded. This is to improve the fail-safety, redundancy and reliability of data systems.

There are several draft versions of acts which have passed the government's legislative procedure and which could become law soon. For example, the *SMART IoT Act* (H.R.2644), which mandates the Secretary of Commerce to conduct a study on the state of the IoT industry to ensure awareness of the presence and danger of IoT devices. Also, the *IoT Cybersecurity Improvement Act of 2019* (H.R.1668), which obliges the NIST to ensure the functions of cybersecurity of IoT devices.

At the level of federal state legislation, California received a new IoT bill (SB-327) with a focus on security of connected devices, which will enter into force on January 1st, 2020. The bill requires manufacturers of any internet-connected device to equip them with reasonable security features. These also include the technical protection of personal data. Per definition, “connected device” means any device, or other physical object that can connect to the internet, directly or indirectly, and that is assigned an IP or Bluetooth address. “Manufacturer” is widely defined as a person who manufactures, or contracts with another person to manufacture on the person’s behalf, connected devices that are sold or offered for sale in California.

JAPAN

Currently, there is no complete regulation on IoT security in Japan. General legal approaches on cybersecurity in Japan are the *Basic Act on Cybersecurity* of 2014, the *Telecommunication Business Act*, and the *Act on the Protection of Personal Information*.

The Japanese cybersecurity act provides the general framework for the responsibilities and policies to enhance nationwide cybersecurity. This includes the protection of critical infrastructures as well. Based on the Basic Act, the National Center of Incident Readiness and Strategy for Cybersecurity was established in 2015.

A revision of the Telecommunication Act in January 2019 allows the National Institute of Information and Communications Technology (NICT) to scan IoT devices such as smart home systems, routers, or webcams with improper password settings and share information about possible threats with third parties, which share the information again with their users.

With the revised Telecommunication Act, it is also possible to establish independent parties, which work as information gathering hubs to manage threats for sensitive information. If one network managed by a such party is attacked, the network access will be blocked, and the attackers’ information will be shared among other networks to prevent them from being attacked in the same way as the initial one.

The concretisation of general legal requirements for IoT device security may be reached through several sublegal acts and guidelines created by the Japanese government. In September 2018, Japan’s Ministry of Internal Affairs & Communication (MIC) amended the technical standard for terminal equipment for IoT security purposes. The amendments apply to devices which are directly connected to Internet Service Providers (ISPs) to protect them from hacker attacks.

Since attacks on IoT devices exponentially increased in the last years, the measures on IoT device vulnerabilities were determined by the necessity of protecting against vulnerabilities for the entire lifecycle of IoT devices and the necessity of organizing the structure to conduct vulnerability assessments. This is done by the promotion of research and development (by studying targeted attacks in detail), acceleration of security measures in the private sector, the strengthening of human resource development (by teaching staff how to handle cyberattacks), and the promotion of international cooperation.

Sector-specific requirements are being set up as well, for, among others, the energy sector by the “Security Guideline on Smart Meter System”. The goal of this guideline is to reduce cyberthreats by influencing the operation of smart meter-systems. The guideline advises operators of smart-meters to establish a management which is responsible for security measures to clarify the relation between the security management and the IT security system of the smart meter. Moreover, it recommends the training of all persons involved in handling the system in a secure way and to introduce to these persons the security measurements of the systems and how to handle threats against the IT security of smart meters. A certification of the cyber protection system, which secures the smart meter, is recommended.

CHINA

The discussion on IT security regulation in China is mainly shaped by the *Chinese Cybersecurity Law* (CSL), which was passed in 2016 and came into force in June 2017. In particular, the law's stipulations for VPN connections from and to China, as well as the regulation of product certification of devices which are used in critical infrastructures drew attention internationally.

The regulation of cybersecurity in China enjoys a relatively long tradition, as the Computer Information System Security Protection Regulations of the People's Republic of China of 1994 already contain corresponding provisions. The most recent and important cybersecurity-relevant law in China concerns the *Chinese Cryptography Law*, which will enter into force on 1st of January 2020. The law prescribes different levels of cryptography, standardisation, and regulations for import and export of cryptographic products.

Compared to the US, the regulation of IoT security in China is quite vague, as there are no special laws dealing with this topic. It is a characteristic of Chinese laws that they can only be regarded as a general legal framework and will mostly not contain any information about implementation or concrete requirements. This is the reason it is possible that many of the current parts of the general Chinese cybersecurity legislation might also be of interest for the security of IoT devices. General and indefinite legal terms allow a broad scope of application for several Chinese security laws. The Chinese legislation is concretized step by step by sublegal norms and through technical standardisation.

.....
The regulation of cybersecurity in China enjoys a relatively long tradition, as the Computer Information System Security Protection Regulations of the People's Republic of China of 1994 already contain corresponding provisions.

Comparison of IoT security regulations in India and EU/Germany

The Indian regulation of IoT security is characterized on the one hand by highly specialised (draft) policies with references to IoT and on the other hand by wide-ranging regulations and more general policies that also touch upon IoT related issues. With the *draft IoT Policy of 2015*, India developed a comprehensive framework to address the development and challenges specific to IoT. However, the draft has not been accepted as an official government policy.

In the EU and Germany, the political and legal requirements have increasingly moved towards IoT, but are not as subject-specific as the *draft IoT Policy of 2015*. The legal frameworks in India tend to include general clauses – similar to German and EU requirements – which cover the topic of IoT (as a side-product) under various aspects, in particular regarding cybersecurity and data protection.

The legal IoT framework in India is primarily covered by the *Information Technology Act of 2000* and the draft of the *Personal Data Protection Bill (2018)*. Both laws highlight the relevance of data protection of IoT devices, which often collect and process large amounts of personal data. In this case, parallels arise in the purpose of IoT regulation in the different countries.

Since the security of personal data is primarily concerned with technical-organisational requirements, indefinite legal terms such as ‘reasonable security practices and procedures’, which the laws do not further specify, are also used in Indian law. This is an inherent consequence of nearly every legal IT regulation: the law itself will hardly be able to cover the contents of the rapid technological development. There are similarities regarding the proposed extra-legal concretisation of legal requirements. The implementation of data security in Indian law is referred to the ISO/IEC 2700X series, similar to the German IT-SiG of 2015.

It is noticeable that the legal requirements for data security of the *IT Act, 2000* only concern „sensitive personal data or information“. In the EU, Art. 32 GDPR goes further by determining the security of the processing of personal data, but also incorporating the severity of the risk for those affected by data processing.

Also the level of (financial) sanctions in case of non-compliance with data security requirements of the IT Act remain behind those of the GDPR: A maximum sum of only 100,000 rupees (approx. 1,270 EUR) is fixed. This is not comparable to the maximum liability sums of the GDPR, where a certain percentage of the whole annual turnover of a company can be imposed.

Imprisonment as a sanction is not provided under EU data protection law, but computer offenses nationally regulated by the EU Member States may be relevant in case of intentional acts and deliberate damage to databases or data processing systems.

In contrast to German and EU law, the *draft IoT Policy 2015* proposes an independent IoT strategy. The policy is to be accompanied by a governance structure and corresponding standards. The governance structure includes a legal framework with regulations adapted to the technological challenges. The proposed advisory and governance committees as well as the program management unit as an executive body, do not have a German or European counterpart yet and are thus difficult to compare with existing structures.

Standardisation is also comprehensively addressed in European IT security law, although not always specifically related to IoT. The draft *IoT Policy 2015* may, in certain aspects, be compared with the EU certification framework, which is being developed based on the rolling work programme of the EU Commission in accordance with the *EU Cybersecurity Act*. Here, ENISA is asked to consult the standardisation organisations regularly for the development of appropriate certification schemes. However, the new EU certification framework is not exclusively tailored to IoT, although it can be assumed that many product categories of the IoT will also be included. Other documents, such as the *National Cybersecurity Policy* of 2013, highlight an intensive interaction between standardisation and policies in India, too.

The *National Digital Communications Policy*, 2018 includes noteworthy approaches as well. In addition to the development of a cybersecurity certification scheme, which correlates with the developments of the *EU Cybersecurity Act*, the policy proposes to set up a register for mobile devices to capture security vulnerabilities, theft, or reprogramming of an (IoT) device. At the same time, monitoring measures for digital communication are proposed. Although such approaches may appear practical, it should be noted that consumer confidence and transparency are key factors in the successful development of the IoT market. Excessive state control and surveillance measures are likely to oppose this development and affect user confidence if in conflict with data privacy.

Regarding the proposal of the Indian *Personal Data Protection Bill* of 2018, there is only little new information compared to the GDPR. The draft emphasises the typical technical-organisational goals of data security, as far as personal data is processed by IoT devices. As noted in the beginning, these technical protection goals are generally uniformly defined in global legal comparison, since they are not substantiated by the law itself, but by rules outside the law such as technical norms and standards.

The background of the image is a complex, light blue maze pattern. The maze consists of many interconnected paths and dead ends, creating a sense of depth and complexity. The paths are formed by darker blue lines on a lighter blue background. In the upper right quadrant, there is a dark blue rectangular box containing white text. The text is arranged in two lines, with the first line being 'STANDARDS' and the second line being 'FOR IOT SECURITY'. The font is a clean, sans-serif typeface.

STANDARDS FOR IOT SECURITY

Standards for IoT Security

Standards are voluntary documents which provide guidance on the design, use or performance of materials, products, processes, services, systems or persons. While they are voluntary in nature, the industry can use them to prove compliance to legislation. In the EU for example, legislation only defines essential requirements and (harmonised) European standards can be used to show compliance. Furthermore, standards are used in business contracts, public procurement or are the basis for certification.

With regards to IoT, standards are essential to achieve interoperability, security, and safety. Compliance with requirements set by regulative provisions can be shown by applying standards which define reasonable security practices. Given the wide range of applications of IoT and the fast pace of technological development, today's global standards landscape for IoT security is fragmented and competitive.²⁸ This is also due to the strong role of de facto standards – developed by single entities or consortia and accepted by the market – as opposed to formal standards which are developed by standardisation organisations.

While gaps in standardisation can be closed by further standardisation, the issue of overlapping standards requires a more difficult reduction of existing standards.

While gaps in standardisation can be closed by further standardisation, the issue of overlapping standards requires a more difficult reduction of existing standards.²⁹ Also, a complex standards landscape raises the costs for small and medium-sized companies in identifying standards relevant to them.³⁰ Hence, early collaboration for the development of international standards for IoT security is crucial.

The following list provides a non-exhaustive overview of important standards and technical specifications for IoT security. The focus of the list is IoT devices. However, given the inherent connectivity of IoT devices, some important standards relating to the IoT systems, processes, and environment level are included here as well.

International

Given the multiple use cases and different layers of IoT, ISO and IEC developed two key standards which provide the common language and orientation in the IoT sphere. Because of this, the two following standards are an important basis:

- **ISO/IEC 30141: 2018, Internet of Things IoT Reference Architecture**
This standard gives orientation for designers and developers of IoT about the various old and new standards applicable to IoT. The reference architecture goes beyond traditional layered frameworks used for IT and developed a Six-Domain Model to help subdivide the IoT system into users, operation and management, application and services, resource access and inter-change, sensing and controlling, and physical entity.³¹
- **ISO/IEC 20924: 2018, Information technology – Internet of Things (IoT) – Definition and vocabulary**
This standard developed a definition of IoT and establishes a set of terms and definitions for a uniform terminology foundation for IoT.

²⁸ Brass, Irina. 2018. "Standardising a Moving Target: The Development and Evolution of IoT Security Standards." p. 4.

²⁹ European Union Agency for Cybersecurity (ENISA). 2018. *IoT Security Standards Gap Analysis*, p. 11.

³⁰ ISO. 2018. "Focus 132: The Cyber Secrets." p. 15 – 23.

³¹ ISO. 2018. "Focus 132: The Cyber Secrets." p. 15 – 23.

With regards to security of IoT devices, currently ongoing standardisation work includes:

- **ISO/IEC 27030 WD, Information technology – Security techniques – Guidelines for security and privacy in Internet of Things (IoT)**

This working draft acknowledges the mentioned challenges of IoT for information security in that they are highly distributed and involve many diverse entities. This implies that there is a large attack surface and a significant challenge for the information security management system (ISMS) to apply and maintain appropriate security controls across the whole system. This standard defines security and privacy controls for stakeholders in an IoT system environment across the IoT system lifecycle.

- **ISO/IEC 24391 NP, Information technology – Security techniques – Guidelines for IoT-domotics security and privacy**

IoT domotics is the IoT system deployed in residential environments to provide services such as home entertainment, home appliance control, home care, and home monitoring applications, where IT, network communication, multimedia, IoT, artificial intelligence may be used. By comparison with general IoT, IoT domotics has some features, such as complex composition, non expert users, and ad-hoc architecture. In accordance, this standardisation effort adapts the general IoT security and privacy principles to IoT domotics, and guides in specific scenarios of IoT domotics. The standard is primarily aimed at IoT-domotics service providers, developers of services and people monitoring or verifying the security and data protection of IoT-domotics.

The following two standards are not specific to IoT devices, but key standards in the overall IoT security landscape:

- **IEC 62443 – Industrial Automation and Control Systems Security**

The IEC 62443 series of standards provides a flexible framework to address and mitigate security vulnerabilities in industrial automation and control systems (IACSs). Its objective is to improve the safety, availability, integrity and confidentiality of IACS components or systems. It builds on established standards such as the ISO/IEC 27000 series. However, it does not only refer to IT systems, but all systems, components, and processes for industrial automation units.

The series has four different elements: general provisions, policies and procedures, system, and components. IEC 62443 elaborates on several concepts, such as security assurance levels, defense-in-depth (coordinated use of security countermeasures), and network zoning/segmentation, and compensating controls (a product takes over security tasks of another in the system).

Several conformity assessment bodies offer certification against standards in the IEC 62443 series.

- **ISO/IEC 27000 series – Information Technology – Security techniques – Information security management systems**

The ISO/IEC 27000 series comprises more than a dozen different standards and comprises some of the most well-known international standards. ISO/IEC 27001 provides the requirements for an information security management system (ISMS). It defines a systematic approach to managing sensitive company information and ways of keeping it secure. It covers people, processes, and IT systems. Even though the first versions of the standards were developed more than 20 years ago, it still represents key mechanisms for organisations to assess their risks, set up mitigating control systems, and continuously evaluate and improve them. Despite this, it cannot be ensured that an organisation which follows all guidelines of ISO/IEC 27000 will successfully develop an IoT device that can also be considered secure.

The following standard is included due to its importance to certification of IoT devices and therefore listed here:

- **ISO/IEC 15408: 2009 - Information technology – Security techniques – Evaluation criteria for IT security**

The international standard ISO/IEC 15408 is also known as Common Criteria for Information Technology Security Evaluation (Common Criteria, CC). It establishes IT security evaluation principles which can be applied to products, components, and systems – different from ISO/IEC 27000 which applied to management systems or organisations. Common Criteria does not lay out requirements for products but only for their evaluation. The intensity and extent of evaluation differ according to seven different evaluation assurance levels (EALs) which the standard defines. Developed originally by public institutions, the Common Criteria are primarily used for products and components of interest to national security (e.g. smart cards). Accordingly, Common Criteria certificates are issued by respective national agencies responsible for security (like the BSI in Germany).

In addition to the ISO/IEC standards which provide the baseline, further standards provide sector-specific standards and specifications (e.g. by oneM2M, 3GPP, etc.). Which are not covered in this publication.

India

The Bureau of Indian Standards (BIS) is India's national standards body which is exclusively authorised to publish Indian standards. Within BIS, the technical committee on *Information Systems Security and Privacy (LITD17)* of the Electronics and Information Technology Division Council (LITDC) is primarily responsible for IoT security standardisation. LITD17 is the mirror committee of subcommittee SC 27 of the ISO/IEC joint technical committee (JTC1) for *Information Security, cyber security and privacy protection*.

BIS has received a proposal to formulate an Indian standard on IoT ecosystem security. The planned standard is devised in four parts:

- **Part 1:** Overview of the IoT ecosystem, its associated domains and security considerations
- **Part 2:** Identification of security objectives and segregation of security requirements in different domains of the IoT ecosystem
- **Part 3:** Definition of security classes of IoT devices and ecosystems, and their applicability for security assessment, evaluation, and certification
- **Part 4:** Outline of an approach and methodology for assessing and evaluating the security of an IoT ecosystem

India actively contributes to the development of ISO/IEC 27030 WD and ISO/IEC 24391 NP as part of ISO/IEC JTC 1/SC 27 WG 4.

Europe

- **ETSI TS 103 645: 2019 – Cybersecurity for consumer IoT**

The European Telecommunications Standards Institute (ETSI) published the technical specification ETSI TS 103 645 V1.1.1 (2019-02) for cybersecurity for consumer IoT.³² ETSI is an independent, not-for-profit, standardisation organisation in the telecommunications industry in Europe with worldwide projection.

The technical specification establishes a security baseline for internet-connected consumer products and provides a basis for future IoT certification schemes. It lists thirteen cybersecurity provisions for consumer IoT products, such as: no universal default passwords, implementing means to manage reports of vulnerabilities, keeping software updated, securely storing credentials and security-sensitive data, making systems resilient to outages, and making it easy for consumers to delete personal data.

Germany

- **DIN SPEC 27072: 2019 – IoT capable devices – Minimum requirements for information security**

The German National Institute for Standardization (DIN) released the specification DIN SPEC 27072 for IoT capable devices – minimum requirements for information security in May 2019. It specifies requirements for connected devices used in a small business-home environment. While the specification is not intended to assure the security of IoT devices, complying with the outlined requirements is believed to reduce the likelihood of common attacks against such devices. Moreover, the specification can support procurement processes and can be used for implementing the planned German IT security marking.

³² It covers products such as connected children's toys and baby monitors, connected safety-relevant products such as smoke detectors and door locks, smart cameras, TVs and speakers, wearable health trackers, connected home automation and alarm systems, connected appliances (e.g. washing machines, fridges) or smart home assistants.



CERTIFICATION OF IOT SECURITY



Certification of IoT Security

Conformity assessment, including testing and certification, is the procedure used to determine that relevant requirements such as legislative provisions or standards are fulfilled. It can take place through manufacturer's self-declaration (self-assessment), third-party assessment by independent and accredited conformity assessment bodies (CABs), or through national authorities.

By applying an appropriate conformity assessment procedure, IoT manufacturers, providers and operators demonstrate that they comply with the requirements such as regarding interoperability, performance, security, and safety.

Security marks or labels – a result of conformity assessment – inform consumers about the security of IoT devices they buy or use. Trusted and easy-to-understand security marks enable consumers to make informed decisions about a matter otherwise too complex for them assess. This shall unleash market forces to drive out unsecure IoT devices. However, for this to work consumers need to be aware of those marks and regard cybersecurity as important for their buying decisions. A fragmented system of security marks is likely to create uncertainty and to reduce consumer trust.

Against the background of international trade of IoT products and services, it would be beneficial to counter an international fragmentation of security marks. The following chapters therefore give an overview of the role of certification in the EU, Germany, and India. Even if legal requirements differ, a harmonised approach of demonstrating compliance through certification based on international standards could facilitate international trade. Accreditation and its proven system of international recognition arrangements could be a basis for internationally trusted IoT security certificates.

This overview focuses on certification based on legal requirements or with the involvement of public authorities. In addition to those listed below, there is of course a wide range of certification schemes (either accredited or not) by private CABs which are not included in this publication.

.....
A harmonised approach of demonstrating compliance through certification based on international standards could facilitate international trade.

India

In India, some IoT devices are covered by mandatory testing and certification of telecommunications equipment (MTCTE). The Department of Telecommunications (DoT) of the Indian Ministry of Communications has established the MTCTE with the *Indian Telegraph (Amendment) Rules, 2017*. The implementation of MTCTE for certain products started on 1 October 2019.

The MTCTE covers all telecom equipment to be sold in India for being connected or capable of being connected to Indian telecom network.³³ It accordingly covers different types of telephones and some IoT devices such as IoT gateways, tracking devices, smart electricity meters, smart watches, and smart cameras. The scope of devices covered is defined through further notifications. Currently, 45 kinds of equipment are intended to be covered.

³³ TEC. 2017. "Procedure for Mandatory Testing & Certification of Telecommunication Equipment".

Exemptions include modules, spare parts, components, test instruments, passive telecom components, and equipment manufactured in India but exclusively meant for export.³⁴ Moreover, presently IoT sensors and inter-sectoral devices with exclusively propriety communication interfaces are exempted too.

The basis for testing are essential requirements specified by DoT's Telecommunication Engineering Centre (TEC). These can include parameters, standards, requirements, or further specifications relating to aspects such as electromagnetic interference (EMI), electromagnetic compatibility (EMC), safety, and security. Regarding security of IoT devices, the essential requirements were not available at the time of writing this publication.

Telecommunications equipment is covered by one the two following certification schemes:

- **General Certification Scheme (GCS)**

Applicants must submit test-wise compliance along with test reports based on essential requirements from designated conformity assessment bodies (CAB) or recognized CAB of partner countries with which a mutual recognition arrangement (MRA) in the framework of the International Laboratory Accreditation Cooperation (ILAC) exists.³⁵ Based on CAB's test report, TEC issues the certificate.

- **Simplified Certification Scheme (SCS)**

Applicants must submit a test report along with a Self-Declaration of Conformity (SDoC) according to parameters laid out in essential requirements. After successful examination by TEC, it issues the certificate.

Equipment which have received the certificate need to be marked accordingly. However, TEC has relaxed this marking requirement for the initial period of six months (i.e. until March 2020). Market surveillance of MTCTE products is carried out by licensed service area field units of DoT.

• Further information can be found on the MTCTE portal at <https://www.mtcte.tec.gov.in/>.

European Union

Certification plays a critical role in increasing trust and security in products and services that are crucial for the EU digital single market.

Certification plays a critical role in increasing trust and security in products and services that are crucial for the EU digital single market. At the moment, a number of different security certification schemes for ICT products exist in the EU.

As mentioned above, the *EU Cybersecurity Act* (CSA) establishes an EU certification framework for ICT digital products, services, and processes. The cybersecurity certification framework enables the creation of tailored and risk-based EU certification schemes but does not introduce operational schemes itself. Certificates will be recognised across all EU member states, thereby easing cross-border trade, and enhancing the understanding of the security features of a product or service. EU cybersecurity certification will be voluntary in the beginning, unless certification is required by EU or Member State law. It is expected that the EU Commission will present a list of mandatory certification schemes until 2023.

³⁴ *Ibid.*, Annexure 1, tables 1, 2 and 3.

³⁵ The acceptance of test reports from accredited labs of ILAC MRA signatories is mentioned as relaxation of the MTCTE procedure and shall be valid until 30 March 2020 as of now.

The process of preparing certification schemes has several stages and involves several stakeholders with different tasks. The CSA cites at this point the European Cybersecurity Certification Group (ECCG), the ENISA Advisory Group, the Stakeholder Cybersecurity Certification Group (SCCG) and the National Liaison Officers Network.

Please refer to the table below for an overview of composition and responsibilities of the three groups:

European Cybersecurity Certification Group (ECCG)	<ul style="list-style-type: none"> • Representatives from EU Member States (from their respective national cybersecurity certification authorities)
Stakeholder Cybersecurity Certification Group (SCCG)	<p>Up to 50 members</p> <p>Comprises representatives from:</p> <ul style="list-style-type: none"> • Academic institutions, consumer organisations, conformity assessment bodies, standard developing organisations, companies, trade associations and other membership organisations. Representatives are selected by the Director General of the EU Commission's Directorate-General for Communications Networks, Content and Technology (DG CNECT) • European Standardisation Organisations (CEN, CENELEC, ETSI) • International Standardisation Organisations (ISO, IEC, ITU) • European co-operation for Accreditation (EA) • European Data Protection Board (EDPB) <p>The SCCG advises the EU Commission and ENISA on strategic issues regarding cybersecurity certification. It assists the EU Commission in preparing the Union rolling work programme.</p>
ENISA Advisory Group	<p>Comprises 33 members from all over Europe</p> <p>The ENISA Management Board sets up the Advisory Group for a term of office of 2,5 years. The composition of the group shall ensure sufficient representation of stakeholders in the work of ENISA.</p> <p>It shall bring issues deemed relevant to the attention of ENISA. It shall be consulted in particular regarding ENISA's draft annual work programme.</p>

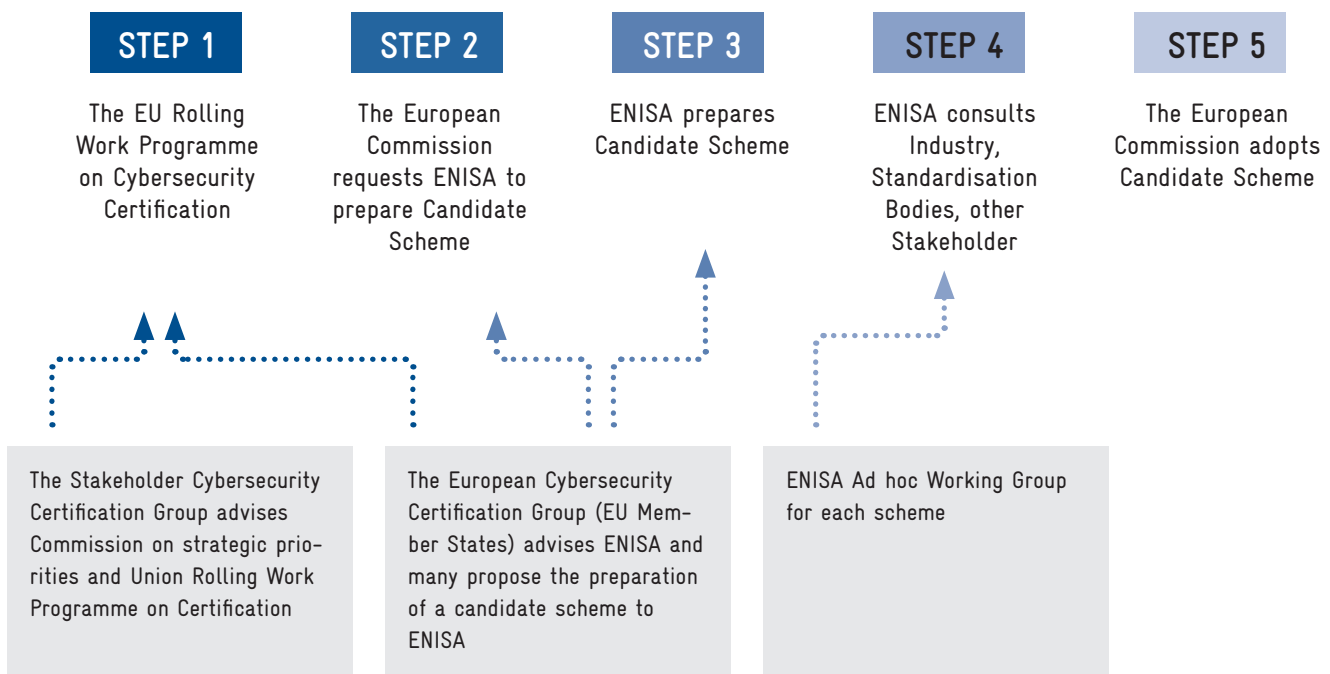
For developing certification schemes, the EU Commission prepares a "Union rolling work program for European cybersecurity certification" which defines the strategic benchmarks which ICT products, services or processes can benefit from when included in a European cybersecurity certification scheme. For this, the EU Commission considers the opinion of the ECCG and the advice of the SCCG.

The first rolling work program is expected to be published by mid-2020 and be updated at least every three years. The following criteria may be decisive for inclusion in the rolling work program:

- Availability and development of national cybersecurity certification schemes covering a specific category of ICT products, services, or processes and, the risk of fragmentation
- Relevant EU or Member State law or policy
- Market demand
- Developments in the cyber threat landscape, and
- Request for the preparation of a specific candidate scheme by the ECCG.

Based on the rolling work programme, ENISA prepares schemes considering the advice from all Member States through the ECCG and receives support from ad-hoc working groups which are set up for this purpose. The ECCG submits non-binding comments on the final draft of the scheme. A final candidate certification scheme is scrutinised by EU Member States prior to the EU Commission’s vote as an Implementing Act (see graph below illustrating the process).

THE LIFECYCLE OF A EUROPEAN CYBERSECURITY CERTIFICATION SCHEME



Graph based on EU Commission (2019): “The EU Cybersecurity Act at a Glance”.

The cybersecurity certification schemes are divided into three assurance levels: “basic”, “substantial” and “high”. The assurance level applied depends on the risk of using the product, as measured by factors of the probability and impact of an incident.

- **Assurance level “basic”:** An evaluation is required at a level intended to minimize the known basic risks of incidents and cyberattacks. Evaluation activities shall include at least a review of technical documentation. This assurance level expected to apply to most consumer IoT devices.
- **Assurance level “substantial”:** An evaluation is required at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. Evaluation activities shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, services, or processes correctly implement the necessary security functionalities. This assurance level is expected to apply to IoT devices for industrial use (Industry 4.0).
- **Assurance level “high”:** An evaluation is required at a level intended to minimize the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. Evaluation activities shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, services, or processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. This assurance level is expected to apply for critical infrastructure.

.....
The assurance level applied depends on the risk of using the product, as measured by factors of the probability and impact of an incident.

The minimum content of a European cybersecurity certification scheme is portrayed in detail in article 54 CSA. Among others, subject matter and scope of the certification scheme, including the type or categories of ICT products, services, and processes covered; a clear description of the purpose of the scheme and how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended user of the scheme; and references to the international, European or national standards applied in the evaluation must be specified.

The CSA distinguishes by certification schemes which allow for self-assessment of conformity by the manufacturer or supplier, and third-party certification (either by conformity assessment bodies or public bodies).

Self-assessment involves the issuing of an EU Statement of Conformity, which states that a specific ICT product complies with the requirements of the European cybersecurity certification scheme. The issuing of an EU Statement of Conformity is only possible for insurance level “basic”.

Third party certification includes all assurance levels and results in the issuance of an EU Cybersecurity Certificate. The responsibility for carrying out the certification for the assurance level “basic” and “substantial” mostly lies with (private) conformity assessment bodies. For the assurance level “high” the national cybersecurity certification authorities are required, either by carrying out certification themselves or through delegation to a CAB (see simplified overview in next page).

ASSURANCE LEVEL	TYPE OF CONFORMITY ASSESSMENT		
<p>Basic (e.g. most smart home devices)</p>	<p>Self-Assessment by Manufacturer or supplier EU Statement of Conformity</p>	<p>Third-party certification (mostly by private conformity assessment bodies, accredited by national accreditation bodies)</p>	
<p>Substantial (e.g. most industrial IoT devices)</p>			
<p>High (e.g. critical infrastructure)</p>			<p>National cybersecurity certification authorities</p>

The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to the CSA, e.g. sufficient independence, technical knowledge and transparency. The accreditation will be issued for a maximum of five years and may be renewed.

For each adopted EU cybersecurity certification scheme, there will be a notification of the conformity assessment bodies which are in charge for the respective certification. The conformity assessment bodies will be published in the *Official Journal of the European Union*.

In case of a certification or a statement of conformity after self-assessment, the following supplementary cybersecurity information must be made publicly available by the manufacturer/provider in electronic form:

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or services
- Period during which security support will be offered to end users, in particular regarding the availability of cybersecurity updates
- Contact information of the manufacturer or provider, and accepted methods for receiving vulnerability information from end users and security researchers, and
- Reference to online sources listing publicly disclosed vulnerabilities related to the ICT product, service, or process and to any relevant cybersecurity advisories.

Germany

The draft *German IT Security Act 2.0* (IT-SiG 2.0) plans to establish a security marking. For the design of the security marking, the Federal Ministry of the Interior, Building and Community (BMI) shall enact a subordinate regulation (decree). The IT security marking shall be subdivided into a declaration by the manufacturer about the IT security features of the product and an official BSI information about security vulnerabilities. The mark can be published on the packaging, the product itself and electronically. Compliance with the requirements of the marking is regularly checked by the BSI.

International

As described above, an important certification scheme for the IT security of products, components, and systems is Common Criteria (based on ISO/IEC 15408).

The Common Criteria certification procedure involves the applicant (manufacturer or distributor), the national certification body (e.g. national cybersecurity agency), and a licenced testing laboratory. At the beginning of the procedure, the applicant together with the certification body and laboratory define the security targets for the specific product or component.

The targets can refer to protection profiles which are pre-defined for certain product types. Protection profiles therefore simplify the development of security targets as general requirements only need to be adapted to specific products. Moreover, they offer users the opportunity to specify security requirements for IT security requirements that manufacturers must meet during the development of a product.

Based on the agreed security targets, the applicant can then enter an evaluation contract with a testing laboratory. The testing laboratory carries out the evaluation according to the defined criteria and issues an evaluation report. Subsequently, the certification body issues a Common Criteria certificate upon successful assessment of the evaluation report.


The international acceptance of Common Criteria certificates is facilitated through multilateral agreements. In the EU, 17 member states have acceded to the agreement of the Senior Officials Group – Information Systems Security (SOG-IS). Certificate producing nations agreed to recognise certificates up to the fourth evaluation assurance level (EAL4) and at higher levels for technical areas approved by the management committee. At the international level, 31 countries have entered the Common Criteria Recognition Arrangement (CCRA) to mutually recognise certificates up to EAL2.

The level of detail and scope of the evaluation depends on the EAL: the higher the EAL, the more intensive the evaluation. For example, EAL 4 and higher include the evaluation of design documents such as source code or hardware blueprints. The efforts for certification vary significantly and the costs can be substantial. The estimated certification costs for a smart meter lie between 150,000 and 1,000,000 Euros.³⁶

The market for Common Criteria certifications is comparatively small. There are only about 30 licensed testing laboratories in Europe and since 1999 only approx. 2000 products have been certified globally.³⁷ Common Criteria are mainly used for devices used by governments for official purposes and critical infrastructure.

³⁶ Kleinhaus. 2019. "Standardisierung & Zertifizierung in der IT-Sicherheit.", *Stiftung Neue Verantwortung*, p. 23.

³⁷ *Ibid.*, p. 24.



**SECURITY OF IOT
DEVICES – DISCUSSION
POINTS FOR THE ROAD AHEAD**

Security of IoT Devices – Discussion Points for the Road Ahead

This paper's goal is to contribute to an informed discussion on regulation and the role of standardisation and certification to ensure the security of IoT devices. During the development of this publication, stakeholders drew attention to the points detailed below.³⁸

- **Aligning regulations internationally, or at least compliance procedures**

Internationally aligned regulatory approaches for security of IoT devices reduce compliance costs for companies and for users. Moreover, exchange on international approaches fosters policy learning and the spread of good practices.

However, different regulatory starting points and policy contexts might make it difficult to reach convergence. Therefore, industry representatives would appreciate a harmonisation at the level of compliance procedures, such as standards. This allows for technical harmonisation even for complying with different regulatory goals. From the perspective of the contributing stakeholders, it is crucial that regulations are technology-neutral and do not impede the development of innovative solutions, i.e. not prescribe certain technological solutions to achieving regulatory objectives. In a fast-changing technological context, mandatory standards carry the risk to be outdated, obstruct innovation, and increase compliance costs for companies.

- **Priority to internationally harmonised and voluntary standards**

Industry representatives highlighted the crucial and enabling role of voluntary and internationally harmonised standards. They enable mutual market access and make standards development more efficient as established good practices codified in international standards can be built upon.

Industry-driven standards and technical specifications are dynamic ways of implementing state-of-the-art technologies and reaching regulatory targets. Given the multi-faceted IoT landscape, IoT standards tend to get fragmented. Industry representatives highlighted the need to counter such a trend, for example by early international exchange on national standardisation activities and giving priority to international standards development. International standards should provide the baseline while further standards would provide sector-specific standards and specifications (e.g. by oneM2M, 3GPP, etc.).

Standardisation needs for IoT devices are seen especially at the protocol and architecture levels (e.g. sensor connectivity, network and gateway layer, management service layer, and application layer) to ensure interoperability and communication between devices. Moreover, standards shall cover the complete process of an IoT device from its design to product retirement, and cybersecurity shall be considered at each stage.

.....
In a fast-changing technological context, mandatory standards carry the risk to be outdated, obstruct innovation, and increase compliance costs for companies.

.....
Industry-driven standards and technical specifications are dynamic ways of implementing state-of-the-art technologies and reaching regulatory targets.

³⁸ These points were mentioned by participants of an Indo-German Expert Exchange on 16 May 2019 in Mumbai and/or at subsequent interactions.

.....
 Industry experts demand flexible conformity assessment which targets processes and approaches.

- **Using flexible certification, internationally recognised**

IoT security is a moving target and static certificates or labels risk being outdated or ineffective. Industry experts therefore demand flexible conformity assessment which targets processes and approaches.

Industry experts emphasised the importance that third-party certification shall not be too time consuming, leading to a longer time-to-market. Otherwise, it could potentially delay the availability of security relevant updates and impede innovation. Stakeholders mentioned their doubts, for example, whether the thorough and therefore costly and time-consuming Common Criteria certification would provide a suitable framework for non-critical IoT devices. It is seen as important that product certification is not only a snapshot at a single point of time but assesses the security of a product over its entire life cycle. If the costs are comparatively high, manufacturers are discouraged to re-certify products.

Moreover, stakeholders underlined that security markings can decrease the information asymmetry between consumers and companies and guide purchase decisions. A precondition is that consumers can understand the underlying criteria of markings. It is important that consumers understand the meaning of a marking as well as its role in the system with the objective to take over responsibilities for maintaining the security of an IoT device. Moreover, consumers need (internationally) well-recognised labels instead of a fragmented and therefore confusing landscape of different approaches. The international accreditation system provides an important tool to establish internationally trusted labels and marks.

- **Agreeing on risk categories and corresponding conformity assessment needs**

Stakeholders stressed that the type of conformity assessment and involved institutions need to depend on the risk of IoT devices. The risk of an IoT device depends on its characteristics (e.g. how easy it is to install patches, how it is powered, how it is connected to other devices, life-span, etc.), intended use (e.g. whether it processes personal information, whether it is used by consumers or industry), and the potential damage (e.g. whether it poses a safety hazard, and whether it affects other IoT devices).

Depending on the risk of an IoT device, the appropriate conformity assessment procedure can be chosen. Similar to the EU Cybersecurity certification framework, an assurance level of 'basic' might only require a self-declaration of conformity by manufacturers while other categories might require the involvement of independent and accredited third-party conformity assessment bodies. Similarly, the approach to market surveillance to check whether IoT devices comply with defined requirements needs to follow a risk-based approach.

The risk categorisation is determined by the chosen criteria and their respective weight. Stakeholders would therefore appreciate an aligned approach to risk categorisation and would appreciate further exchange on this. Moreover, the risk categorisation approach needs to be updated regularly to react to new technological developments and changed threat scenarios.

- **Developing joint approaches to product liability issues**

An important question relates to the liability of manufacturers, distributors, conformity assessment bodies, and consumers in case of incidents with a certified product. Stakeholders pointed to the fact that certification alone does not exonerate manufacturers from their responsibilities. The specific liabilities, however, need to be defined – especially with the blurring lines between product safety and security. For example, are consumers responsible for the damage of an incident if they did not update their IoT device regularly? At what point can a manufacturer of an IoT device stop providing important security updates?

Given the crucial role of secure and regularly updated software for a device's functioning, stakeholders ask for discussing the need of software being regulated as a product rather than a service. Furthermore, liability questions relate to responsibilities for informing users of IoT devices about known vulnerabilities and disclosing security breaches.

Conclusion

This discussion paper highlighted the multi-faceted implications of IoT security: its relevance to privacy, product safety and liability, and national security. Quality infrastructure, especially standards and conformity assessment, plays a crucial role in ensuring IoT security. India and Germany have decided to explore aligned responses in this emerging field. This strengthens consumer confidence and protection and eases bilateral economic cooperation. With global value chains, it is imperative to harmonise regulatory frameworks. The emerging area of IoT device security provides an opportunity to cooperate early on and find joint approaches to this global challenge.

The regulatory frameworks for IoT security in India, Germany, and the EU vary in their breadth and depth between. A common element is the importance to define and regularly review what is considered as reasonable security practices. Standards can provide important guidance in this regard and provide companies with options on how to comply with regulations.

Under the framework of the Indo-German Working Group on Quality Infrastructure, it would therefore be beneficial to conduct regular exchanges on the development and review of guidelines and standards that represent reasonable security practices for IoT security which supports both countries' industries in fulfilling their legal obligations and following state-of-the-art approaches. The Indo-German Working Group on Quality Infrastructure brings together the relevant experts from the public and private sectors and facilitates joint efforts.

Stakeholders point to the fact that conformity assessment needs to be adequate to the risk category of IoT devices. Therefore, it is suggested to engage in an Indo-German dialogue on risk categorisation approaches and exchange on conformity assessment schemes for the respective risk profiles.

This discussion paper stressed the importance of international standardisation. As part of their bilateral cooperation, India and Germany should strengthen their bilateral exchange on national standardisation activities and intensify their cooperation at the international level. This would support harmonised international standards development and closing of current gaps regarding IoT device security.

This discussion paper shall provide input for further discussions around IoT device security. Therefore, further cooperation topics may arise from the subsequent exchanges and will be suggested to the Indo-German Working Group on Quality Infrastructure.

.....
The emerging area of IoT device security provides an opportunity to cooperate early on and find joint approaches to this global challenge.

References

- Baldauf, Sebastian. 2019. “The digital (GDPR-compliant) office – a technical experience report.” DS 2019, 130.
- Bitz, Gunter. 2017. “Data-protection-desert IoT.” DuD 2017, 636.
- Brass, Irina. 2018. “Standardising a Moving Target: The Development and Evolution of IoT Security Standards.”
- Conrad, Sebastian. 2017. “Artificial intelligence – risks for data protection.” DuD 2017, 740.
- Department of Telecommunications (DoT). 2018. “National Digital Communications Policy.” <http://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf>.
- DIN-SPEC 27072:05-2019. . “Information Technology - IoT capable devices - Minimum requirements for Information security.” <https://www.din.de/en/getting-involved/standards-committees/nia/din-spec/wdc-beuth:din21:303463577>.
- Djeffal, Christian. 2019. “IT-Security 3.0: The new IT-basic-protection.” MMR 2019, 289.
- Eckert, Claudia, and Michael Waidner. 2018. “Safety and security.” Digitalisierung, 275.
- European Commission. 2019. “The EU Cybersecurity Act at a Glance.” <https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-glance>.
- European Telecommunications Standards Institute (ETSI). 2019. “CYBER - Cyber Security for Consumer Internet of Things.” ETSI TS 103 645 V1.1.1. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.
- European Union Agency For Network and Information Security (ENISA). 2018. “Good Practices for Security of Internet of Things in the context of Smart Manufacturing.” <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>.
- . 2018. “IoT Security Standards Gap Analysis.”
- International Organization for Standardization (ISO). 2019. Architecting a Connected Future. <https://www.iso.org/news/ref2361.html>.
- . 2018. “Focus 132: The Cyber Secrets.”
- InternetSociety. 2017. “IoT Security for Policymakers.”
- Kiparski, Gerd, and Thomas Sassenberg. 2018. “Internet of Things – current developments and industry particularities for connected cars, eHealth and co.” CR 2018, 596.
- Kipker, Dennis-Kenji. 2020. “Cybersecurity: Legal Handbook.” Munich: Beck.
- . 2019. “IT-Security Act 2.0 – draft bill published.” MMR-Aktuell 2019, 415455.
- . 2019. “Japan – Draft of a “cyber/physical security framework” published.” MMR-Aktuell 2019, 413345.
- Kipker, Dennis-Kenji, and Dario Scholz. 2019. “ The IT-Security Act 2.0.” MMR 2019, 431.
- . 2019. “EU – New proposal for establishing a new European Centre of Competence for Cybersecurity.” MMR-Aktuell 2019, 410979.

- Kipker, Dennis-Kenji, and Sven Müller. 2019. "International Regulation of Cybersecurity – Legal and Technical Requirements." MMR-Aktuell 2019, 414291.
- Kleinhans, Jan-Peter. 2019. "Standardisierung & Zertifizierung in der IT-Sicherheit." Stiftung Neue Verantwortung.
- Küll, Carolin. 2019. "Data protection in networked products and in digital marketing of the health sector." A&R, 2019, 51.
- Ministry of Communications and Information Technology. 2011. "Reasonable Security Practices and Procedures and Sensitive Personal Data or Information."
- Ministry of Electronics & Information Technology (MeitY). 2018. "Draft Personal Data Protection Bill."
- . 2015. "Draft Policy on Internet of Things."
https://meity.gov.in/writereaddata/files/Revised-Draft-IoT-Policy_0.pdf.
- . 2000. "Information Technology Act."
- . 2013. "National Cyber Security Policy." https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.
- Muppiri, Chandrasekhar. 2019. "Public-Private Partnerships in Indian Industrial IoT: A Set of Policy Recommendations to Improve Cyber Security."
- National Institute of Standards and Technology (NIST). 2019. "Core Cybersecurity Feature Baseline for Securable IoT Devices draft."
- Organisation for Economic Co-operation and Development (OECD). 2016. "The Internet of Things Seizing the Benefits and Addressing the Challenges." No. 252. June.
- Ritter, Steve. 2019. "The new Californian Law for Security of Networked Devices." MMR 2019, 3.
- Schmitz, Barbara. 2018. "The farewell to the personal reference." ZD 2018, 5.
- Schmon, Christoph. 2018. "Product Liability of Emerging Digital Technologies." IWZR 2018, 254.
- Spies, Axel. 2018. "California: New IoT-law signed." ZD-Aktuell 2018, 06313.
- Telecommunication Engineering Centre (TEC). 2017. "Procedure for Mandatory Testing & Certification of Telecommunication Equipment."
- . 2019. "Technical Report. Recommendations for IoT/M2M Security." January.
<http://tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20Iot%20M2M%20Security.pdf>.
- United Kingdom Department for Digital, Culture, Media and Sport (UK-DCMS). 2018. "Mapping of IoT security recommendations, guidance and standards to the UK's Code of Practice for Consumer IoT Security."
https://aioti.eu/wp-content/uploads/2019/06/DCMS_Mapping_of_IoT_Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf.
- Weber, Rolf. 2017. "Liability in the Internet of Things." EuCML 2017, 207.

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1 - 5
65760 Eschborn, Germany
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

On behalf of the



Federal Ministry
for Economic Affairs
and Energy