Security and Privacy of Resource-Constrained Devices

Pier Giorgio Chiara [0000-0002-9444-3480]*

PhD Candidate
University of Luxembourg — University of Bologna — University of Turin
Law, Science and Technology, Rights of Internet of Everything
Horizon 2020 - Marie Sklodowska-Curie ITN EJD
piergiorgio.chiara@uni.lu
https://www.last-jd-rioe.eu/

Abstract. Recent adversarial attacks have been shown IoT devices weaknesses due to their limited computing power. Given also their ubiquitous presence, lower costs and limitations in keeping security measures up-to-date, resource-constrained devices represent a growing risk for the security of IT infrastructure. The scope of the research is to investigate the weaknesses of resource-constrained IoT devices. The methodology for the investigation is the legal analysis of existing legal frameworks regulating IoT cybersecurity and data security; afterwards it will be carried out a critical evaluation of the existing best practices. This critical analysis should face the twofold challenge of increasing transparency and trust in resource-constrained systems. Users and companies are two faces of the same coin: accountability of data collectors and user awareness are crucial in the security and data protection debate. Thus, a comprehensive overview of the relevant legal frameworks and guidelines would increase the understanding of risks of the users, whilst data controllers (especially of small and medium enterprises) may have an instrument to implement properly security measures

Keywords: Security · Privacy · IoT.

1 Theoretical Premise

This section will be devoted to look deeper into the rationales and aims of privacy and data protection, on the one hand, and security, on the other hand, into different perspectives, considered as a spectrum stretching from ethical and legal understandings towards more technical approach.

The right to privacy is closely related to the right to data protection[1, 2], they may often overlap, albeit with distinct scopes and rationales[3–5]: the former is conceived to protect people's "opaqueness", whilst the latter concerns the "transparency" of the collection and process of personal data[6]. I would

assume that an analysis on the right to privacy may not fail to consider also data protection's related aspects, given their intertwined relation.

The approaches all together lead to a holistic vision of what constitutes privacy, data protection and security. The goal here is not to provide an exhaustive survey of the philosophies behind those concepts, but rather to structure the most relevant themes in the literature by focusing on the underlying interests of privacy, data protection and security in the field of resource-constrained devices.

Moreover, in the realm of IoT, a reflection on group privacy and collective data protection seem appropriate[7]: emerging digital technologies, by processing, linking and merging (big) data, are able to create new datasets, ready for inferential analytics and profiling. "Rather than a unique data subject whose informational self-determination is specifically under attack, individuals are more often targeted as a member of a group, whereas they can even ignore being a part of that group on the basis of a set of ontological and epistemological predicates that cluster people into multiple categories"[8].

2 State of the Art

Nowadays, the Internet of Things (IoT) represents the next step towards digitalization, considering the wide range of IoT applications that have been developed and deployed in the recent years.

Objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and/or about the status of the surrounding environment[9].

The devices that are meant to be connected within the IoT network show different capabilities and features having regard of computational power, mobility, size, complexity, dispersion, power resource, placement, and connectivity patterns[10]. Historically, the devices connected to the internet could have been grouped into a homogeneous class, i.e. fully capable computers or peripherals with endless source of power, characterized by large and quite expensive hardware[10]. This classification is no longer true within the IoT network, which combine together devices with limited CPU, memory and processing power (e.g., pressure sensors)[11] and devices with powerful processors, large memory and replenishable sources for energy (e.g., smartphones). These applications require low-cost hardware to be economically feasible, and they need to be small[12]. Also, recalling[13], one should consider that is unlikely to draw a comprehensive overview of the huge class of embedded systems' hardware components since they are less standardized than hardware for personal computers[8]. Others layers of complexity are brought by the intrinsic nature such devices and services which operate on different local and global networks, are governed by diverse technical and international legislative standards and developed by different manufacturers[14].

IoT resource-constrained devices are likely to challenge many principles of data protection and security. Identification technologies are a crucial component of trusted communication in the IoT, but they may pose risks to users' privacy

in IoT context[15]. Data controllers can draw inferences from these data[16]. Discriminatory treatment can also result from inferential analytics and linkage of disparate records[17], motivating limitations on user profiling. Moreover, individual control over personal data, as claimed by the work of the Article 29 Working Party (all of WP29 guidelines have been formally endorsed by EDPB during its first preliminary meeting), is virtually impossible in the IoT context due to the features of these systems[16].

Furthermore, in many IoT resource-constrained devices, deployed in order to meet the various application requirements, privacy and security have emerged as crucial challenges because on the one hand the systems have not been designed to have effective security features[18], involving therefore cyber-security issues[19]; on the other hand the deployment of IoT resource-constrained devices poses a threat to data (or information) security, namely the protection of information (and information systems) from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability[20].

Following a risk-based approach (the higher the risk, the more rigorous the measures that the controller or the processor needs to take), the level of security shall be assessed, according to art. 32 GDPR, having regard to the state of the art, through the adoption of appropriate technical and organizational measures, equally covering the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

In order to consider reliable and compliant such IT networks and systems components, several security risk assessment methodologies and frameworks have been developed[21], with the aim of helping data controllers in evaluating security risks.

The project considers data controllers of SMEs and users as two sides of the same coin, within the IoT ecosystem. A further development may also consider the applicability of this framework to certification mechanisms issued by competent Data Protection Authorities (DPAs), by turning therefore the initial bipartite relation into a tripartite one.

The choice to focus solely on SMEs revolves around the understanding that these actors, in order to be compliant and protected, face more efforts and difficulties than big companies[22][23]. The 2019 Senseon report points out that nearly half of SMEs interviewed perceive investing in cyber security as a net cost: “it is clear that they struggle to find value from their security stack or products they use”[24]. Moreover, the Australian government carried out a survey with a dramatic scenario. SMEs are the target of 43% of all cybercrimes; 22% of small businesses that were breached by the 2017 Ransomware attacks were so affected they could not continue operating; 33% of businesses with fewer than 100 employees don’t take proactive measures against cyber security breaches; 87% of small businesses believe their business is safe from cyberattacks because they use antivirus software alone; Cybercrime costs the Australian economy more than 1 bllion annually[25][26].

3 Research Questions

The research questions are grouped under three expected results that the research should achieve. Nonetheless, it should be stressed that there is a twofold difficulty in drawing a legal analysis in this field. Thus, relevant academic literature is still poor and emerging digital technologies lack as yet the legal certainty and clarity on sector regulations.

Firstly, it is necessary to analyse the weaknesses of resource-constrained IoT devices to understand the extent to which these new technologies represent a risk, rather than a resource, for society. Therefore, this investigation will take the form of a risk analysis of the IoT bounded-resources.

Thus, in this first part of the project the research questions could be framed as follows: How could IoT resource-constrained de-vices be technically and legally defined? What encompass the definition of "weakness" in the security context of IoTs? To what extent the constrained nature of these devices represent a security risk?

Furthermore, the second part of the project, namely the analysis of legal framework regulating IoT security, addresses mainly a general question: what is the applicable legal framework for ensuring security in IoT context? Indeed, it is sufficient framing the concept of security into information security and cyber security? Are there relevant extra-EU legal framework which refer to IoT security[1]?

Thirdly, IoT technologies are likely to challenge many principles of data protection, producers and data controllers should be stimulated to go above and beyond the strict legal requirements of existing regulations in order to elaborate privacy enhancing systems and services that endeavor to reach, among all, the principle of transparency (recital 58, GDPR).

Therefore, the adoption of appropriate security framework and best practices for resource con-strained devices raises further interrogatives: what are the relevant soft law instruments in the context of resource-constrained devices security? how can these instruments be implemented in order to be easily understood by both users and entrepreneurs?

4 Methodology

4.1 Analysis of the Weaknesses of Resource-Constrained IoT Devices

Setting the context Firstly, it has to be developed the notion of resource-constrained IoT devices. Given the resource constraints, together with the self-

[1] UK would enforce a mandatory labelling system to determine the level of security of an internet-enabled device [27]; US federal legislation on data protection and privacy seems not prepared to face the challenges posed by IoT [37, 40] -according to several scholars, federal data protection and privacy laws are to some extent not adequate to face the challenges posed by IoT, even though some States, like California, have taken countermeasures through a bottom-up approach [28].

organization and short-range communication, these technologies always resort to the cloud for outsourced storage and computation[29]. This process, involving cyber-sensors with limited energy and storage, brings several security and privacy threats. Indeed, adversaries can actively intercept or manipulate data, or passively monitor data transmission[30]. The exhibition of significant differences in available execution environments, processing, and storage capabilities would add an extra layer of difficulty. In conclusion, to compose a diverse collection of individual elements, a structured approach is needed to uniformly and transparently deploy application components onto a large number of heterogeneous devices[31].

Risk analysis An evaluation of security risks within the IoT ecosystem[2] will be carried on taking primary guidance and structure from the ENISA methodology.

This part shall look deeper into the different steps of a privacy risk assessment process, by carrying out a critical analysis of the methods provided for by existing relevant guidelines and standards.

4.2 Analysis of Legal Frameworks Regulating IoT Security

Notion of information security The concept of information security underpins the understanding of security oriented towards the protection of data and information[32]: the so-called CIA triad (confidentiality, integrity and availability) typical of the computer security is expanded to include other principles such as non-repudiation, authenticity, accountability and auditability. The legal analysis of this section will mainly address, as regulative instruments, the GDPR and the Regulation on non-personal data.

GDPR The EU Regulation 2016/679 states, at article 32, that controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.Standards urgently require further specification and implementation into the design and deployment of IoT technologies for users to make an informed decision if they want to use their services[33].

Regulation on non-personal data The EU Regulation 2018/1807 constitutes a framework for the free flow of non-personal data in the European Union. The expanding Internet of Things represent one of the major sources of non-personal data. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics; nonetheless, whether technological improvements may convert anonymised data into personal data, such process of data has to be treated under the rules of the GDPR.

[2] [22], 17-33: definition of the processing operation and its context; understanding and evaluating impact; definition of possible threats and evaluation of their likelihood; evaluation of risk.

Notion of cyber-security Cyber-security generally refers to the ability to protect or defend the use of cyber-space form cyber-attacks[34]. It, therefore, encompasses a broad range of risks governance. The level of safety of individuals and businesses in cyber-space is relevant as a value in itself and in view of national security perceived as a critical sphere where everyone is involved. Thus, this understanding may gather three lines of action such as the critical infrastructure protection, the digital market development and the safeguarding of the fundamental rights and freedoms.

The legal analysis of this section will mainly focus on relevant legal measures that aim to boost the overall level of cybersecurity in the EU, such as: the Cybersecurity Act, namely the EU Regulation 2019/881 on ENISA (the European Union Agency for Cy-bersecurity) and on information and communications technology cybersecurity certification,the "eIDAS" Regulation or Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market and the "NIS" Directive on security of network and information systems.

The intertwined relation between cybersecurity and information security

Interrelation with privacy by design and privacy by default Privacy by design and privacy by default are closely interlinked with security of processing (article 32 GDPR), another essential GDPR requirement, since they together fall within the broad notion of "privacy engineering, i.e. embedding privacy requirements into the information systems' design and operation"[35].

Critical analysis of the current PETs adopted Data minimization[3] and other various GDPR principles such as privacy by design and by default can in several instances be achieved by the use of security and privacy enhancing technologies[36][35]. Therefore, pseudonimisation[4], encryption as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of compromised data), anonymization techniques and other PETs (such as VPN, onion routing, DNS security extension, transport layer security and private information retrieval) should be used in order to achieve information privacy goals. However, relevant literature showed that PETs may be flawed as a well-motivated hacker would be able to re-identify the individual [33].

[3] Data minimisation is one of the core principle of the European data protection framework, stating that personal data should only be processed if the purpose of the processing cannot be fulfilled by other means.

[4] [37],pseudonymization , 1744: pseudonymization is a common tool to impede the identification of an individual through her personal data: such data can no longer be attributed to her without using additional information, which must be kept separately. The risk of re-identification is higher with pseudonymized data than with anonymized ones: as Ohm noted, "just as "anonymize" fails to acknowledge reversible scrubbing, "pseudonymize" fails to credit robust scrubbing".

- *Pseudonimisation, anonymization and encryption* Moreover, as noted in [19, 38] data are generally encrypted or anonymized only later on, in the cloud server: aggregated data are of real value at the very first stage, before being compressed and sent to the cloud for being processed. Thus, these techniques usually take place when the valuable information have already been extracted from the data. When the data generated by Internet of Things devices are collected anonymously or directly anonymized, either on the device or in the cloud, GDPR will not be applicable to profiling based on these data. However, the Article 29 Working Party identified the risk of re-identification of personal data as one of the main six data protection challenges for the Internet of Things [39, 37, 40].

- *DPIA requirement* Moreover, the General Data Protection Regulation states that where a type of processing is likely to result in a high risk for the rights and freedoms of individuals, which would likely be the case of IoT, the controller shall carry out a DPIA, i.e. [41]: according to Article 29 Working Party, several IoT applications are likely to pose significant concerns with regard to individuals' right to privacy and data protection; therefore, they require a DPIA [42]. Nevertheless, as noted in [15], "the uncertain value of personal data generated and processed by IoT devices and services necessarily limits the scope of risks that can be foreseen, and thus reduces the protection actually offered by DPIAs". Also, the DPIA should not be confused with the security risk assessment (as per the first phase). Indeed, while, the latter is a crucial step of the former, a DPIA considers several other requirements related to the personal data processing, going beyond security.

4.3 Security Framework and Best Practices for Resource Constrained Devices

Following the evaluation of the level of the risk, attained in section 3.1, the research project focuses on the analysis of appropriate security measures for resource-constrained devices.

Knowledge for this part of research will be collected, as a main resource, from ENISA's works[22]. According to article 32 of GDPR, two categories of measures will be taken into account: organizational and technical ones. Afterwards, these bipartion will be further framed into subsections, explaining how each measure relates to specific provisions of GDPR. Each subsection measures, both technical[5] and organizational[6], will be consider in a scaled classification per risk level. In order to achieve scalability, it is assumed that all measures described under the low level are applicable to all levels. Similarly, measures presented under the medium level are applicable also to high level of risk. Measures presented under the high level are not applicable to any other level of risk [22].

[5] [22], 33-39: security management; incident response and business continuity; human resources.

[6] [22], 39-48: access control and authentication; logging and monitoring; security of data at rest; network/communication security; back-ups; mobile/portable devices; application lifecycle security; data deletion/disposal; physical security.

5 Project Proposal

The PhD thesis will investigate, under the lens of regulations and standards in force nowadays, how the security of personal data processing and cybersecurity can be lawfully enforced by data controllers (especially of SMEs) in resource-constrained IoT systems with a security risk management plan compliant and, on the other side how user's trust can be enhanced. The aim of the project is therefore to provide a legal analysis of the broad notion of security of processing and cybersecurity, and its intertwined relation with both data controllers and users, within the IoT ecosystem, in order to bridge the gap between the legal provisions and their understanding as well as the perception of risk. The former (data controllers) may benefit from this work made up by legislative texts, standards, guidelines and code of conducts in developing a security risk management plan, the latter (users) will better understand the risks connected to the security of their devices and of the processing involving their data. Data protection as transparency is perceived as a crucial issue, even more with growing spread of ubiquitous IoT applications, since most privacy enhancing tools (PETs) are useless if they are not used properly or if they are not implemented in an automated way: thus, "new approaches to transparency of data collections and accountability of data collectors and user awareness are crucial the privacy debate" [43–45]. Furthermore, as expressed in [46], transparency may contribute to the accountability of data controllers.Limitations on user oversight and on transparency in management of security of processing are likely to ease data breaches and undermine trust, by hampering therefore the significant potential of IoT devices.

Furthermore, I will get in touch with local companies to identify suitable case-studies where to apply and evaluate the effectiveness of the project.

6 Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD "Law, Science and Technology Rights of Internet of Everything" grant agreement No 814177.

References

1. Fuster, GG and Hijmans, H (2019). The EU rights to privacy and personal data protection: 20 years in 10 questions. In International Workshop 'Exploring the Privacy and Data Protection connection: International Workshop on the Legal Notions of Privacy and Data Protection in EU Law in a Rapidly Changing World'. Brussels Privacy Hub. Law, Science, Technology and Society Research Group.
2. Kokott, J and Sobotta, C (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law, 3(4), 222-228.

3. Docksey, C, and Hijmans, H (2019). The Court of Justice as a Key Player in Privacy and Data Protection. European Data Protection Law Review, 5(3), 300-316.
4. Elliott, D (2019). Opinions: Data Protection Is More Than Privacy. European Data Protection Law Review, Volume 5, Issue 1, 13-16.
5. Lynskey, O (2014). Deconstructing data protection: the 'added-value'of a right to data protection in the EU legal order. International and Comparative Law Quarterly, 63(3), 569-597.
6. Pagallo, U (2017). The Group, the Private and the Individual: A New Level of Data Protection? In Taylor, L, Floridi, L, Van der Sloot, B (eds) Group Privacy: New Challenges of Data Technologies, Philosophical Studies Series 126. Springer International Publishing, 161.
7. Taylor, L, Floridi, L, Van der Sloot, B (eds) Group Privacy: New Challenges of Data Technologies, Philosophical Studies Series 126. Springer International Publishing, 3
8. Pagallo, U, Durante, M, Monteleone, S (2017). What is new with the internet of things in privacy and data protection? Four legal challenges on sharing and control in IoT. In Data protection and privacy:(In) visibilities and infrastructures (pp. 59-78). Springer, Cham., 71
9. Commission Staff Working Document (2016). Advancing the Internet of Things in Europe,accompanying the document communication from the Commission to the European Parlia-ment, the Council, the European economic and social committee and the committee of theregions. Digitising European Industry Reaping the full benefits of a Digital Single Market.
10. Rayes, A, Salam, S (2017). Internet of things—from hype to reality. Springer.
11. Bormann, C, Ersue, M, Keranen, A (2014). Terminology for constrained-node networks. Internet Engineering Task Force (IETF): Fremont, CA, USA, 2070-1721.
12. Stapko, T (2011). Practical embedded security: building secure resource-constrained systems. Elsevier, 85
13. Marwedel, P (2018). Embedded system design. Springer, 126
14. Wachter, S, Mittelstadt, B and Floridi, L (2017). Transparent, explainable, and accountable AI for robotics.
15. Wachter, S (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Computer law & security review. Elsevier, 34,3,436-449.
16. Eskens, S (2016). Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to This Form of Personal Data Processing, and How Should It? Available at SSRN 2752010
17. Barocas, S and Selbst, AD (2016) Big data's disparate impact. Calif. L. Rev. HeinOnline, 104, 671
18. Li, S and Song, H and Iqbal, M (2019) Privacy and security for resource-constrained IoT devices and networks: Research challenges and opportunities,Multidisciplinary Digital Publishing Institute
19. Weber RH (2010) Internet of Things–New security and privacy challenges. Computer law & security review, 26,1. Elsevier, 23-30
20. Glossary of Computer Security Resource Center, National Institute of Standard and Technology. Voice: information security.US Department of Commerce
21. ENISA. Inventory of Risk Management / Risk Assessment Methods and Tools. Url=https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory
22. ENISA (2016). Guidelines for SMEs on the security of personal data processing.Url=https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

23. CISCO (2018). Small and Mighty - How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats. Url=https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf
24. SENSEON (2019). The State of CyberSecurity SME Report. Url=https://www.cbronline.com/wp-content/uploads/dlmuploads/2019/06/Senseon-SME-Report-2019-Web.pdf
25. Australian Government (2018). The Small Business Cyber Security Best PracticeGuide. Url=https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-guide.pdf
26. BBB (2017). State of Cybersecurity among Small Businesses in North America. Url=http://saginllc.com/wp-content/uploads/2017/10/CybersecurityFINALLoResEmbargoed.pdf
27. Towers-Clarks C (2/05/2019). UK To Introduce New Law For IoT Device Security. Forbes. Url= https://www.forbes.com/sites/charlestowersclark/2019/05/02/uk-to-introduce-new-law-for-iot-device-security/154741e7579d
28. Robertson A (28/09/2018). California just became the first state with an Internet of Things cybersecurity law.The Verge.Url=https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law
29. Zhou, J, Cao, Z, Dong, X, and Vasilakos, AV (2017). Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine, 55(1), 26-33.
30. Ning, H, Liu, H, and Yang, LT (2013). Cyberentity security in the internet of things. Computer, 46(4), 46-53.
31. Vögler, M, Schleicher, J, Inzinger, C, Nastic, S, Sehic, S, and Dustdar, S (2015). LEONORE–large-scale provisioning of resource-constrained IoT deployments. IEEE Symposium on Service-Oriented System Engineering, 78-87.
32. Nieles, M, Dempsey, K, Pillitteri, VY, (2017). An Introduction to Information Security. NIST Special Publication.
33. Wachter S (2018). The GDPR and the Internet of Things: a three-step transparency model. Law, Innovation and Technology, 10, 2. Taylor & Francis, 266–294.
34. Kissel, RL, (2013). Glossary of Key Information Security Terms. NIST Interagency/Internal Report (NISTIR) - 7298 Rev. 2.
35. ENISA (2018). Recommendations on shaping technology according to GDPRprovisions:Exploring the notion of data protection by default. Url=https://www.aepd.es/media/docs/recomendations-on-shaping-technology-according-to-GDPR-provisions-2.pdf
36. Voigt, P and Von dem Bussche, A (2017). The eu general data protection regulation (gdpr), a Practical Guide. 1st Ed., Cham: Springer International Publishing,Springer.
37. Ohm P (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA l. Rev.57. HeinOnline, 1701 and ff.
38. Xiao, Q and Gibbons, T and Lebrun, H (2009). Rfid technology, security vulnerabilities, and countermeasures. Supply Chain the Way to Flat Organisation,IntechOpen.
39. Article 29 Data Protection Working Party (2014). Opinion 8/2014 on the Recent Developments on the Inter-net of Things.Url=ttps://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223en.pdf
40. Peppet, SR (2014). Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. Tex. L. Rev., 93,85. HeinOnline

41. CNIL (2018).Privacy Impact Assessment – Application to IoT Devices. Url=https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf
42. Article 29 Data Protection Working Party (2017). Guidelines on Data Protection Impact Assessment(DPIA) and determining whether processing is "likely to result in a high risk" for the pur-poses of Regulation 2016/679. Url=https://ec.europa.eu/newsroom/article29/item-detail.cfm?itemid=611236
43. Weber RH (2015). Internet of things: Privacy issues revisited. Computer Law & Security Review, 31, 5. Elsevier, 618-627.
44. European Commission (2013). Internet of Things, Reports. Url=https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation
45. Mauritius Declaration on the Internet of Things (2014). 36th International Conference of Data Protection and Privacy Commissioners. Url=http://www.privacyconference2014.org/media/16596/Mauritius-declaration.pdf
46. Article 29 Data Protection Working Party (2010). Opinion 3/2010 on the principle of accountability. Url=https://www.dataprotection.ro/servlet/ViewDocument?id=654