Extending an LGPD Compliance Inspection Checklist to Assess IoT Solutions: An Initial Proposal

Ivonildo Pereira[1], João Mendes[2], Davi Viana[2], Luis Rivero[2], Waldemar Ferreira[1], Sergio Soares[1]

[1]Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Caixa Postal 785150732-970 Recife, PE - Brazil

[2]PPGCC- Universidade Federal do Maranhão (UFMA)
Caixa Postal 322 – CEP.: 65080 – 040 – São Luís - Maranhão.

{ipgn,wpfn,scbs}@cin.ufpe.br, jpm.mendes@discente.ufma.br

{davi.viana,luis.rivero}@ufma.br

Abstract. *Society has become more dependent on technology, so investments in information security have become essential. In Brazil, the General Data Protection Law (Lei Geral de Protecão dos Dados - LGPD) legislates information security management. This work aims to propose an instrument to evaluate the adequacy of IoT solutions regarding the LGPD. The proposal evaluation took place in a private institution linked to industrial innovation. The proposed mechanism can assist professionals in verifying the LGPD adequacy in IoT projects. The study identified LGPD compliance defects in an IoT solution deployed in several industries all over the 23 Brazilian states. However, the results cannot be generalized since we only evaluated it in a single company and one software solution. Replications are needed to identify whether these results apply to other companies and solutions.*

1. Introduction

Nowadays, technology plays a central role in modern society. One technology is gaining momentum in the industry, the Internet of Things (IoT). Garg and Dave [Garg and Dave 2019] define IoT as mechanics to establish connections between devices through the Internet. So IoT devices can connect the physical world to the digital world. Devices like sensors and actuators can collect information from the physical world. This information can be stored and processed by any computer. However, information in IoT solutions may involve personal data, so this is sensitive information.

Considering this scenario, the concern about protecting people's data has grown over the years. Central and State Governments in many countries have enacted laws and regulations to promote personal data protection [Wachter 2018]. A new law has recently been sanctioned in Brazil addressing this issue. The General Law on Personal Data Protection, Law No. 13.709 of 14th August 2018, gives the Brazilian population rights and guarantees how organizations must collect and process personal data, whether by physical or digital means. This regulation brings excellent benefits, allowing greater security of personal data, and non-compliance with the law leads to penalties [Pinheiro 2020]. Without regulation, it would be easier to misuse personal data and excess data collection and

processing beyond what is necessary. It could cause inconvenience to individuals who had their data collected [de Souza et al. 2020].

Data protection laws (including the LGPD) strongly impact any IoT solution [de Oliveira et al. 2019]. Since IoT devices can access sensitive data, thus it requires protection instruments. Nowadays, any data protection instrument must be under the basements and principles defined by the LGPD. In many cases, it is challenging to comply with the LGPD since it does not provide technical definitions regarding the required protection. The law specifies only good practices, leaving it to IoT creators to produce mechanisms to ensure that any sensitive data accessed by the equipment is protected.

In light of the foregoing, this work presents a checklist to verify the adequacy of IoT solutions with the LGPD. Our solution extends a checklist to assess general solutions regarding the LGPD [Mendes et al. 2021]. Unlike the original checklist, our extension considers only those facets specific to the IoT context.

2. Checklist for evaluating IoT solutions

Mendes et al. [Mendes et al. 2021] proposed a checklist to evaluate any information system. However, this instrument was only tailored to general LGPD fundamentals. In singular scenarios, more technical analysis is necessary. For instance, considering the LGPD's good security practices, it mentions that data controllers must create mechanisms for data protection. Such scenarios are recurring when IoT devices are involved. In addition, many authors report vulnerabilities and challenges in protection methods for IoT devices [de Oliveira et al. 2019, Ribeiro and Nakamura 2019, Bernardi et al. 2020]. Considering what was said, an extension of the Mendes et al. [Mendes et al. 2021] checklist was developed, targeting projects involving IoT. In this way, IoT analysts will be able to carry out a complete evaluation of their system.

Table 1 presents an example of the checklist items. Due to space limitations, we cannot present here the complete checklist. However, it is available online[1]. Our checklist extension contains 27 extra items, being categorized into three parts, namely:

- **Data security**: It is related to the protection of personal data.
- **Physical security:** It is related to the physical part of the device, considering the functionalities, protection against physical access, and ambient conditions.
- **Access to the device**: It is related to controlling access to the device, allowing only authorized persons.

Table 1. Example of the proposed checklist

Cat.	items	Recommendations
DS-04	Do devices use protection techniques to perform secure communication?	When sharing data between devices, protection techniques need to be implemented.
DS-06	Does the device properly route data to its destination?	Carry out checks to identify whether data is only being forwarded to its intended destination.
DS-09	Does the device receive security updates?	Security updates fix flaws, and the faster those flaws are fixed, the risk of intrusion decreases.

Our checklist was developed as a spreadsheet template. Other authors also adopt this approach on the same topic [Mendes et al. 2021]. This spreadsheet allows evaluators

[1]https://bit.ly/3vahZJC

to inspect IoT projects' information. Each checklist item has three options: **Yes**, **No**, or **Not applicable**. Option **Yes** means the evaluated system complies with this checklist item. Option **No** means the system is not in conformity with the item. Finally, option **Not applicable** means the item property does not influence the evaluated system.

Figure 1 exemplifies the process of filling out the proposed checklist. In this example, code item **DS02** was evaluated as No. So, evaluators may consider the item's recommendations to make their IoT project adherent to the LGPD.

Data security					
CODE	ITEMS	ANSWER	DEGREE OF SEVERITY	COMMENT	RECOMMENDATIONS
DS01	Is the device certified to prove quality standards?	yes			Using certifications proves that the device has quality and safety levels determined by the regulations. It is essential to have a certificate, such as Anatel Certification.
DS02	Is the device safe from "brute force" attacks and abusive login attempts?	No	SEVERE		A brute force attack is a way to gain privileged access through numerous attempts. One solution is to create a mechanism to block users after several invalid access attempts.

Figure 1. Checklist structure

The meaning of each column in Figure 1 is as follows:

- **Code**: An identification for each item. Each Code has the initials of its category followed by a number. For example, DS01 is the first item in the Data Security category;
- **Items**: The description of a checklist's item. Typically, a question;
- **Answer**: This field must be fulfilled by the evaluator's judgment of the item;
- **Degree of severity**: It is a way for evaluators to judge the level of nonconformity with the LGPD. The severity ranges from Moderate, Severe, or Catastrophic. The severity grade is adapted from [Nielsen 1994].
- **Comments**: A field where evaluators can take notes;
- **Recommendations**: It presents recommendations to solve the system's nonconformity.

3. Evaluation results

Participants in this research first assessment were employees of a private innovation institute linked to industrial innovation. The evaluation was carried out in a project that provides an IoT-based solution for industrial companies where personal and IoT equipment data are processed. Our investigation tool was made available so they could apply it to the projects they were working on at that time. Then, we held a focus group [Debus 1994] with the participants. They reported the checklist brought some benefits, such as identifying neglected safety situations and easily finding security flaws. Participants also suggested changes to improve the structure and suggestions for new extensions, such as cloud network systems. In addition, the evaluations the participants carried out in the industry system through the checklist were analyzed. Then, a debate was held on each checklist item, identifying 11 system security defects. Therefore, the checklist was able to identify real problems in an industrial environment.

4. Conclusion and Future Works

To operationalize a mechanism for verifying the compliance of IoT projects with the LGPD, we propose a checklist. This checklist was proposed based on the specific characteristics of IoT devices. The checklist is an extension of another checklist focused on

verifying compliance with the LGPD in software projects. Together, the original checklist and the extension help analysts and consultants verify LGPD compliance before, during, and after the development of software projects where IoT devices consume data.

The proposed checklist was evaluated through the perception of professionals working on IoT projects in a private industrial innovation institute. In this evaluation, according to the professional's perception, the proposed checklist was able to help professionals in the verification of the adequacy of the LGPD in projects involving IoT. Future work should evaluate the checklist applied to new IoT-based software projects and companies to assess the checklist in different contexts.

References

Bernardi, E., Miyake, M. Y., dos Santos, A. S., Merichelli, M. P., Pereira, M. J., and Polkorny, M. (2020). Brazilian scenarios for smart cities deployment from public policies perspectives. In *2020 IEEE International Smart Cities Conference (ISC2)*, pages 1–8.

de Oliveira, N., Gomes, M., Lopes, R., and Nobre, J. (2019). Segurança da informaçao para internet das coisas (iot): uma abordagem sobre a lei geral de proteçao de dados (lgpd). *Revista Eletrônica de Iniciação Científica em Computação*, 17(4).

de Souza, J. S., Abe, J. M., de Lima, L. A., and de Souza, N. A. (2020). The general law principles for protection the personal data and their importance. *arXiv preprint arXiv:2009.14313*.

Debus, M. (1994). Manual para excelencia en la investigación mediante grupos focales. In *Manual para excelencia en la investigación mediante grupos focales*, pages 97–97.

Garg, H. and Dave, M. (2019). Securing iot devices and securelyconnecting the dots using rest api and middleware. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pages 1–6.

Mendes, J., Viana, D., and Rivero, L. (2021). Developing an inspection checklist for the adequacy assessment of software systems to quality attributes of the brazilian general data protection law: An initial proposal. In *Brazilian Symposium on Software Engineering*, pages 263–268.

Nielsen, J. (1994). Usability inspection methods. In *Conference companion on Human factors in computing systems*, pages 413–414.

Pinheiro, P. P. (2020). *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD*. Saraiva Educação SA.

Ribeiro, S. L. and Nakamura, E. T. (2019). Privacy protection with pseudonymization and anonymization in a health iot system: Results from ocariot. In *2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE)*, pages 904–908.

Wachter, S. (2018). Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr. *Computer law & security review*, 34(3):436–449.