Analysis of business processes compliance with LGPD

Abstract. News about data leaks of private and confidential data are being reported with increasing frequency. To mitigate these issues, governments have taken actions to ensure that companies raise their investments and the actions related to user's data security and privacy. Laws were created, like the European General Data Protection Regulation (GDPR) and the Brazilian law called LGPD (Lei Geral de Proteção de Dados, in portuguese, or General Law of Data Protection), which define the privacy rights on user data and establishes penalties to the companies which do not comply with the law. Data privacy and security, which are fundamental non-functional requirements for many socio-technical systems, became a priority among the problems faced by many companies. These systems support business processes that are of fundamental importance in a compliance program with these laws and to balance transparency on the services provided. This tutorial will discuss the importance of developing privacy-aware systems and business processes and present a method to obtain LGPD compliance in business processes. In particular, LGPD4BP (LGPD for Business Process) - a method composed by an evaluation questionnaire and a modelling method supported by a modelling patterns catalog - will be presented to the audience.

1   Objective

Since data privacy and data security became a priority among the problems faced by many companies, software systems should be compliant with privacy laws. To develop or acquire a system, it is necessary to know the requirements that this system must meet, that is, what the system needs to do, what is its scope and what functionalities it must present. To define such characteristics, it is necessary to analyze the business processes to be supported by the system under construction because it is necessary to clearly understand which process activities will be automated. Accordingly, business processes are of fundamental importance in a compliance program with data protection laws. The goal of this tutorial is to detail the fundamentals of privacy in software intensive products and services [1], discuss the privacy concern in business processes and present the LGPD4BP method [2] proposed to evaluate and model business processes in compliance with LGPD [3].

2   Outline of Topics

- Privacy in software intensive products and services : Privacy foundations (history, definition, privacy vs. security, Personal information vs. Sensitive information); Privacy by Design and by Default; Privacy concepts (Fair Information Practice Principles - FIPP and Privacy-Enhancing Technologies - PET); Privacy-related problems.
- The Brazilian privacy law LGPD: Definition, principles, subjects' rights and the lawful basis for data processing.

- Business Process Modeling: Definition, overview of the main elements of BPMN (Business Process Modeling and Notation) and examples.
- Overview of the LGPD4BP method and exercises.

3 Target audience

This tutorial is suitable for industrial practitioners, researchers as well as students who are interested (beginners) in understanding privacy in software intensive products and services, and business processes compliance with LGPD. No prior skills are required.

4 Presenters' bios, affiliations and e-mails

Mariana Peixoto is a post-doc researcher at the Center of Informatics of the Universidade Federal de Pernambuco (CIn-UFPE), Brazil, since 2021. She earned a Ph.D. in Computer Science from UFPE. Her research interests are Privacy Requirements Engineering, Legal Compliance and Agile Software Development. Email: mmp2@cin.ufpe.br.

Diogo Santos is a Master student at CIn-UFPE, Brazil, since 2020. His research interests are Software Engineering, Privacy and Software Testing. Email: decs@cin.ufpe.br

Jéssyka Vilela is Adjunct Professor at CIn-UFPE. She earned a Ph.D. in Computer Science from UFPE. Her main research lines include Safety-Critical Systems, Software Engineering, Information Security and Privacy. Email: jffv@cin.ufpe.br.

Carla Silva is an Associate Professor at CIn-UFPE. She earned a Ph.D. in Computer Science from UFPE. For the past five years, she has been researching topics on privacy requirements specification, legal compliance and agile practices in safety-critical systems. Email: ctlls@cin.ufpe.br.

Acknowledgements

We would like to thank Eric Araújo for developing the LGPD4BP method.

5 Tutorial presentation

The tutorial will be presented on-line and in Portuguese.

References

1. PEIXOTO, C.; SILVA, C. Especificando requisitos de privacidade com linguagens de modelagem orientadas a objetivos. No XXXII Simpósio Brasileiro de Engenharia de Software (SBES), v. 24, p. 112–121, 2018.
2. ARAÚJO, E.; VILELA, J.; SILVA, C.; ALVES, C. Are My Business Process Models Compliant With LGPD? The LGPD4BP Method to Evaluate and to Model LGPD aware Business Processes. In: Simpósio Brasileiro de Sistemas de Informação (SBSI) , 2021.
3. BRASIL. Decreto n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.