# Towards a Model-based Regulatory Compliance Checking of Customer Agreements: A Case Study *

Octavio Martín-Díaz[2], Carlos Müller[2], José María García[1,2], Pablo Fernández[1,2], and Antonio Ruiz-Cortés[1,2]

[1] Smart Computer Systems Research and Engineering Lab (SCORE)
[2] Research Institute of Informatics Engineering (I3US)
Universidad de Sevilla, Spain
{omartindiaz,cmuller,josemgarcia,pablofm,aruiz}@us.es

**Abstract.** Services in cloud computing are used under the legal terms defined in their customer agreements. Providers have to specify their terms considering applicable regulations. However, varying terminologies make checking regulatory compliance and other analysis operations difficult to generalize and automate. In this paper, we present a case study for checking the compliance of the Google Maps customer agreement with the European General Data Protection Regulation (GDPR). To do so, we use a reference model to obtain the models for both documents, and check their regulatory compliance. Finally, we also discuss the challenges for automation found in this case study.

**Keywords:** Customer Agreements · Regulatory Compliance · Automated Analysis.

## 1 Introduction

Providers must take into account the legal aspects of cloud-related contracts, commonly known as service agreements or, more generically, customer agreements (CA), which include not only the corresponding service level agreement (SLA), but also the terms of service, the privacy policy, and the acceptable use policy, among other elements.

Traditionally, automated CA analysis has focused on SLAs, where objectives play a fundamental role in monitoring whether they are fulfilled in order to obtain compensations in case of violations [13]. Recent efforts also propose analysis operations for pricing and billing terms [8], but only some of them try to operationalize other elements, such as terms of service or privacy policies, to name a few.

* This work has been partially supported by the following grants: PID2021-126227NB-C21, PID2021-126227NB-C22, TED2021-131023B-C21, and PDC2022-133521-I00 which are funded by MCIN/AEI/10.13039/501100011033 and "ERDF a way of making Europe"; and grant PYC20 RE 084 US, which is funded by Junta de Andalucia/ERDF,UE.

Among works on compliance, [1,2,3,4,5,6,7,11,14] present differences in terminology and country-related regulations that, in turn, prevent providers from agreeing on a common model as foundations for their CAs. Furthermore, since legal claims depend on applicable jurisdictions and/or regulations, ensuring regulatory compliance and other analysis operations is much more challenging. In [9], we approached these challenges by devising a common reference model[3] to specify CAs that will support such operationalization while allowing the mapping between the reference model and the terminology usually found in cloud service providers' CAs.

This paper presents a preliminary work consisting of a case study for checking the compliance of the Google Maps customer agreement with the European General Data Protection Regulation (GDPR). To do so, we used our reference model to obtain the models for both documents. Then, we compared both model instances to check their regulatory compliance.

Challenges have been found in this case study. First, the management of the different versions of a CA. Second, the variability of structure and terms used in CAs from different providers. And finally, the comparison of models under the conditions of the previous challenge.

The remainder of this paper is organised as follows. Section 2 presents the reference model we elaborated to provide a common terminology. Section 3 shows how we instantiated our model within the case study comprising GDPR and Google Maps CA. Next, Section 4 discusses the checking of regulatory compliance based on comparing such models and the challenges we have found. Next, Section 5 briefly reviews the related work. Finally, Section 6 presents our conclusions and future work.

## 2 Reference Model

In [9] we presented a reference model for customer agreements, which was based on several guidelines and recommendations [3,7,11]. In the literature and cloud providers' documents, "service agreements" and "customer agreements" (CA) can be commonly used as synonyms that describe a binding between providers and customers.

From a legal perspective, the key point is considering such a binding as a "contract", which is enforceable in law courts. Therefore, we use "contract" as a key element of our proposed CA reference model. They mostly comprise the service-level agreement (SLA), terms of service, privacy policies, and acceptable use policies.

Among them, the "Privacy Policy" (PP) refers to regulations on customer data management (that is, data subjects in GDPR), as Figure 1 indicates. The key elements that we represent in our model are the following:

– "Data integrity" considers security certification, encryption, and recovery management.

[3] Note this reference model was corrected and updated after being published, so that compositions were changed to specializations, as shown in Figure 1.

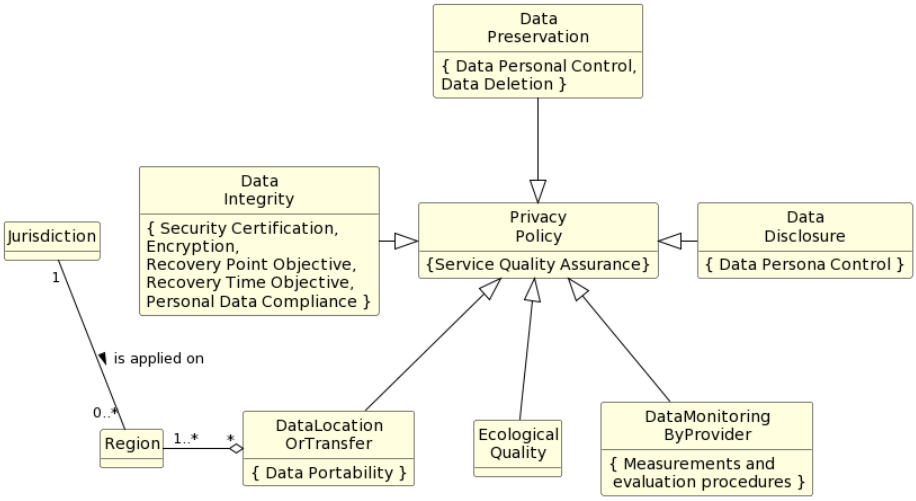


**Fig. 1.** Reference model for privacy policy.

- "Data preservation" includes strategies for actions regarding personal data control and data deletion.
- "Data disclosure" refers to the provider's attitude to sharing personal data with third parties. Personal data cannot be usually disclosed except in court requests, although options vary widely by jurisdiction.
- "Data location or transfer" includes data portability, encryption, and backup location.
- "Ecological quality datacenters" refers to datacenters powered by a neutral carbon or renewable power supply.
- "Data monitoring" by providers includes measurement and evaluation procedures.

## 3 Case Study Modelling

In the following, we present how we have modelled our case study. We first discuss how we represent GDPR instantiating our reference model.

The resulting model will be the framework against which we want to compare other providers to check their regulatory compliance. In our case, we analyse Google Maps CA to model its PP compliance with GDPR.

### 3.1 GDPR Model

Figure 2 showcases the main model devoted to the General Data Protection Regulation (GDPR) principles. Note that, in this preliminary work, we do not

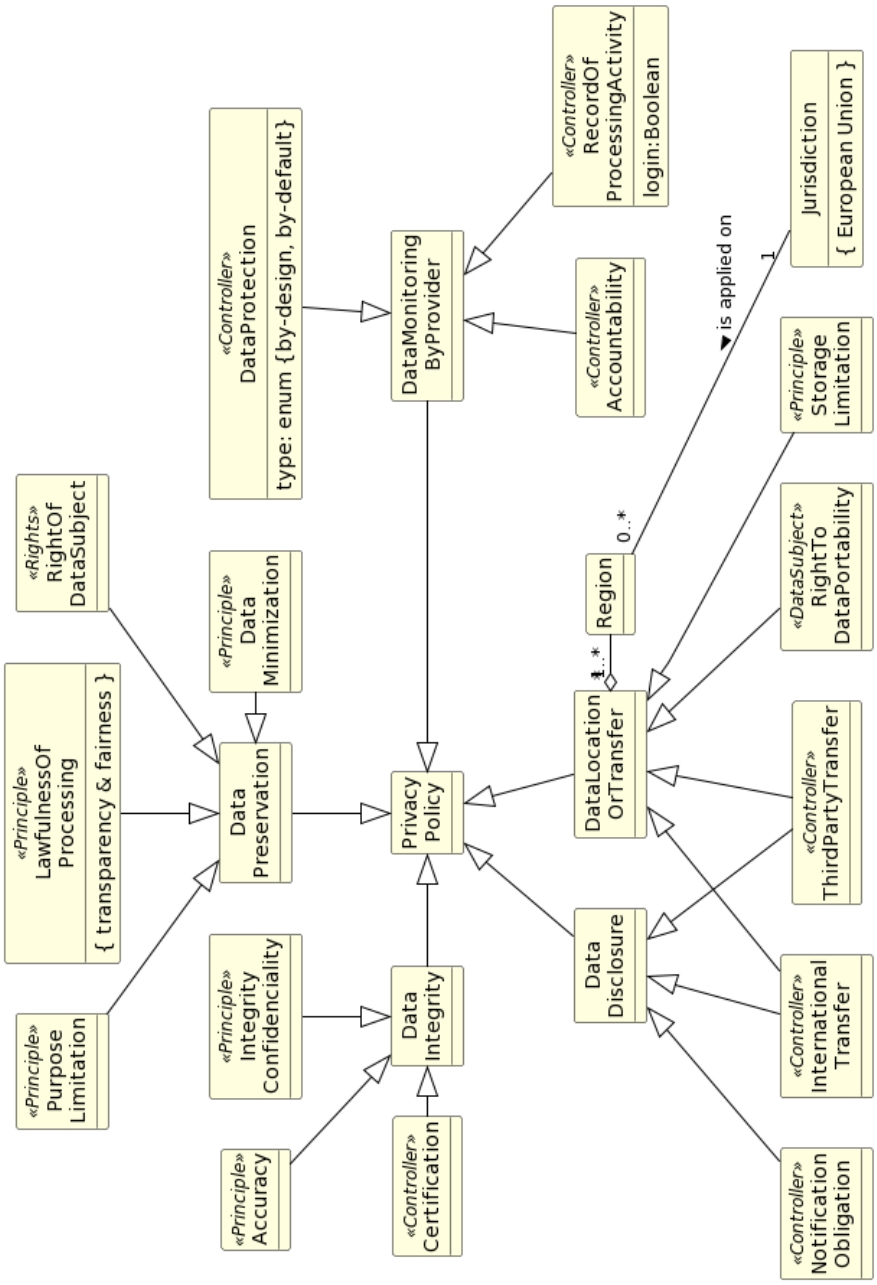


**Fig. 2.** General model for the General Data Protection Regulation (GDPR).

cover all its articles, but we provide some details with respect to process-related lawfulness and data subject rights.

In this model, the GDPR principles are subclasses arranged around the main PP elements of the reference model, with stereotypes denoting several GDPR aspects, such as the following *principles*:

- "Lawfulness of processing" of personal data includes fairness and transparency. The policies for this principle include additional legal obligations, contract performance, vital and public interest, consent by data subjects, a definition of legitimate interest, and also other considerations for special cases depending on the nature of the data to be processed.
- "Purpose limitation" by which personal data must not be further processed beyond their original purpose.
- "Data minimisation" by which the personal data must be processed to the extent to which it is just needed for fulfilling their purpose.
- "Accuracy" by which the personal data must be kept up to date, erased, or rectified,
- "Right of data subject" includes rights to rectification, erasure (i.e. right to be forgotten), access, data portability, object, file complaints, or obtain information transparently.
- "Storage limitation" by which personal data must be kept no longer than needed.
- "Integrity and confidentiality" by which the security of personal data must be guaranteed, increasing the data quality.

In addition, all organisations and companies, either public or private, which manage personal data in the EU must have a *controller*, the stakeholder responsible under the law for achieving compliance with GDPR. Their responsabilities shown in Fig. 2 are:

- "Data protection" by which privacy policy must be tackled, by default or specific design.
- "Record of processing activities" in order to guarantee data monitoring.
- "Accountability" by which the controller must be able to respond those requests by data subjects or supervisory authorities with regard to GDPR compliance.
- "Third-party transfer" and "International transfer" must have into account policies from both data disclosure and data location. In addition, "Data portability" and "Notification of obligation" are considered as rights of data subjects. Moreover, GDPR imposes data from public organizations to be located in data centers physically located in the EU or, if not, ruled on EU directives.
- "Certification" is related to data integrity in a way that the controller must follow the available standards to guarantee GDPR compliance.

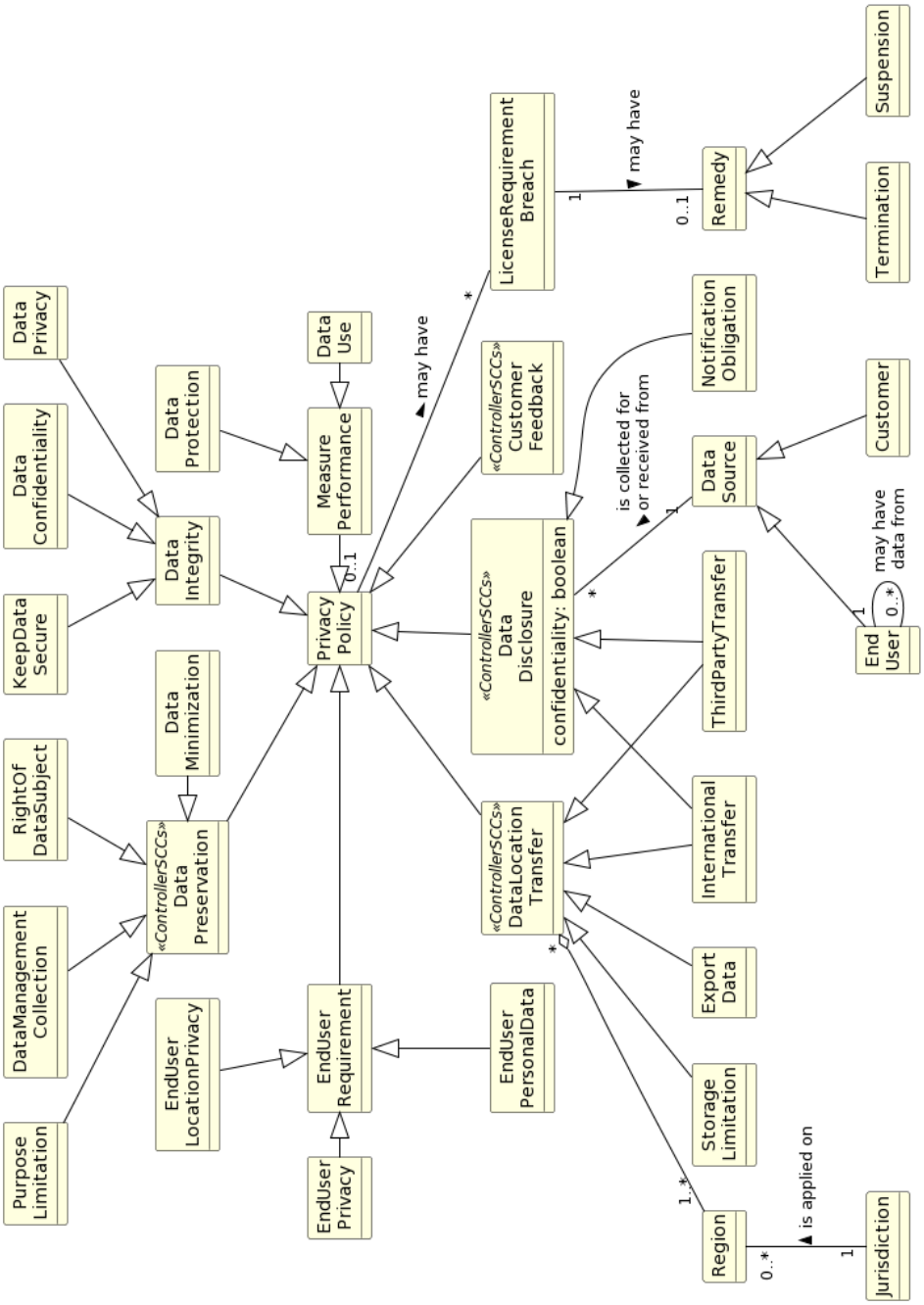


**Fig. 3.** Model for Google Maps privacy policy.

### 3.2 Google Maps Model

In this section, we present the model for the *License Agreement* of the Google Maps platform. It was obtained from the Google privacy policy and also the Google Controller privacy policy, specifically defined for being compliant to EU regulations.

Figure 3 shows the model for Google Maps privacy policy, whose elements are arranged as subclases around the PP elements in the reference model, including the following:

- "End-user requirements" since Google Maps customers can have their own end users, so there are requirements regarding end-user personal data, privacy, and location.
- "Data disclosure" involves restrictions on data sources, which can be either Google Maps customers or their end users. Optionally, confidentiality of disclosed data may be needed.
- "Data preservation", including data management and collection, and rights of data subject.
- "Data location and transfer", whose terms can differ according to jurisdiction, taking specifically GDPR into account.
- "License requirement breach", instead of indemnifications, optionally associated with a remedy, just as described in the reference model.
- "Data integrity" which includes data privacy, and data confidentiality, and specific methods to keep data secure.
- "Measure performance" which includes data protection and data use.
- "Customer feedback" as the need to register the customer's point of view on the use of the tool.

In addition, Google introduces the "SCC controllers", which stands for *standard contractual clauses* in order to regulate the controller relationships, since this stakeholder is a GDPR requirement.

## 4 Discussion on Regulatory Compliance

In order to check the regulatory compliance of Google Maps with respect to the GDPR, we need to compare their models, both obtained from our reference model, shown in Figures 2 and 3.

When visually comparing these models, the compliance result was positive, but with some remarks to be pointed out. First, Google Maps includes several privacy policies regarding end users, customer feedback, and remedies for breaches which are not referred to in GDPR. Regarding principles such as data minimization, purpose limitation, and storage limitation, the policies are broadly defined, so even though they are compliant in principle, a deeper analysis should be carried out in order to realise to which degree they are actually fulfilled because of the amount of data collected by Google.

Therefore, instantiating and comparing these models are tasks that would benefit from a certain degree of automation, hence making it possible to automatically check regulatory compliance and other analysis operations.

However, one of the main problems we faced within this case study was the distance between CAs, regulations and our reference model, both in their terminology and the structure. Even though our reference model was based on several sources which had already made some efforts to manage the commonality among different customer agreements, we still needed to align the elements of all models to be able to compare them and perform the compliance checking.

In summary, automating these operations seems to require a human-expertise review to obtain a proper model for the customer agreement or regulation. Therefore, there are some challenges to face:

- Define a reference model able to tackle variability both in terminology and relationships among different elements of models, not to mention version tracking of customer agreements and regulations.
- Operationalization for checking the compliance to a given jurisdiction or regulation, and other operations by means of comparing models, taking advantage of novel approaches in areas such as generative artificial intelligence, natural language processing, machine learning and semantic technologies.

## 5 Related Work

Regarding privacy policies and their compliance with different regulations, [1] presents a systematic analysis and proposes a Combined Privacy Law Framework (CPLF) including key principles for privacy policies and individual rights, which constitutes the basis for a *Privacy by Design* approach, which has been adopted by the GDPR.

In [12], it is proposed a method for managing GDPR compliance in business processes. Their approach to the GDPR model is fully operational, since its authors try to check whether a business process have all the necessary to fulfill the GDPR requirements from an operative point-of-view, and offers a method so that business processes can be updated in order to achieve such compliance.

A more generic approach is [10], a business process compliance checker, based on the *compliance by design* methodology. Their work has evolved so that compliance is defined as a relationship between the formal representation of a process and the formal representation of the regulation. These formalizations and their checking are rested on rule-based logic reasoning.

Regarding with automating the compliance, there are some works which introduce how to automate the GDPR compliance in cloud-hosted services [5,6] and online healthcare [4] by applying timed transition systems, blockchain, and smart contracts, respectively.

In [2] a review of several approaches to compliance checking is presented in the area of building environments. In [14] a similar approach in healthcare building design is presented.

## 6 Conclusions

In this paper, we have presented a case study for checking the regulatory compliance. To do so, we have obtained the models for the General Data Protection Regulation (GDPR) and Google Maps customer agreement, both based on the reference model presented in [9], which enabled the terminological alignment of customer agreements, so that both providers and customers can specify and analyze legal aspects of cloud services. As future work, we plan to analyze how ontology alignment, natural language processing and machine learning approaches can help to automatize compliance checking and other analysis operations based on a fully-fledged reference model.

## References

1. Aljeraisy, A., Barati, M., Rana, O., Perera, C.: Privacy Laws and Privacy by Design Schemes for the Internet of Things. ACM Computing Surveys **54**(5), 1–38 (6 2022). https://doi.org/10.1145/3450965
2. Amor, R., Dimyadi, J.: The promise of automated compliance checking. Developments in the Built Environment **5**, 100039 (3 2021). https://doi.org/10.1016/j.dibe.2020.100039
3. Badger, L., Bernstein, D., Bohn, R., de Vaulx, F., Hogan, M., Iorga, M., Mao, J., Messina, J., Mills, K., Simmon, E., Sokol, A., Tong, J., Whiteside, F., Leaf, D.: US Government Cloud Computing Technology Roadmap. Tech. rep., National Institute of Standards and Technology, Gaithersburg, MD (10 2014). https://doi.org/10.6028/NIST.SP.500-293, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf
4. Barati, M., Aujla, G.S., Llanos, J.T., Duodu, K.A., Rana, O.F., Carr, M., Ranjan, R.: Privacy-Aware Cloud Auditing for GDPR Compliance Verification in Online Healthcare. IEEE Transactions on Industrial Informatics **18**(7), 4808–4819 (7 2022). https://doi.org/10.1109/TII.2021.3100152
5. Barati, M., Rana, O.: Checking GDPR Compliance for Cloud-based Services. In: 2021 IEEE World Congress on Services (SERVICES). pp. 2–2. IEEE (9 2021). https://doi.org/10.1109/SERVICES51467.2021.00013
6. Barati, M., Theodorakopoulos, G., Rana, O.: Automating GDPR Compliance Verification for Cloud-hosted Services. In: 2020 International Symposium on Networks, Computers and Communications (ISNCC). pp. 1–6. IEEE (10 2020). https://doi.org/10.1109/ISNCC49221.2020.9297309
7. Bradshaw, S., Millard, C., Walden, I.: Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services. International Journal of Law and Information Technology **19**(3), 187–223 (9 2011). https://doi.org/10.1093/ijlit/ear005
8. Garcia, J.M., Martin-Diaz, O., Fernandez, P., Muller, C., Ruiz-Cortes, A.: A Flexible Billing Life Cycle for Cloud Services Using Augmented Customer Agreements. IEEE Access **9**, 44374–44389 (2021). https://doi.org/10.1109/ACCESS.2021.3066443
9. García, J.M., Martín-Díaz, O., Muller, C., Fernandez, P., Ruiz-Cortés: A Common Reference Model for Cloud Services Customer Agreements. In: XVII Jornadas de Ciencia e Ingeniería de Servicios (JCIS). Santiago de Compostela, Spain (2022)

10. Governatori, G., Shek, S.: Regorous: A business process compliance checker. In: ACM 14th International Conference on Artificial Intelligence and Law (ICAIL). pp. 245—246 (2013). https://doi.org/10.1145/2514601.2514638
11. Hans Graux, Jos Dumortier, Patricia Ypma, Jasmine Simpson, Peter McNally, Marc de Vries: Digital Agenda for Europe Standards terms and performance criteria in service level agreements for cloud computing services. Tech. rep., European Union, 2015 (2013). https://doi.org/10.2759/07446
12. Matulevičius, R., Tom, J., Kala, K., Sing, E.: A Method for Managing GDPR Compliance in Business Processes. In: Advanced Information Systems Engineering. CAiSE 2020. pp. 100–112. Springer (8 2020). https://doi.org/10.1007/978-3-030-58135-0_9
13. Müller, C., Fernandez, P., Gutierrez, A.M., Martín-Díaz, O., Resinas, M., Ruiz-Cortés, A.: Automated Validation of Compensable SLAs. IEEE Transactions on Services Computing (2018). https://doi.org/10.1109/tsc.2018.2885766
14. Soliman-Junior, J., Tzortzopoulos, P., Baldauf, J.P., Pedo, B., Kagioglou, M., Formoso, C.T., Humphreys, J.: Automated compliance checking in healthcare building design. Automation in Construction **129**, 103822 (9 2021). https://doi.org/10.1016/j.autcon.2021.103822