Published in: Proceedings of the IEEE CLOUD Conference, 2018, San Francisco

A Knowledge Representation of Cloud Data controls for EU GDPR Compliance

Lavanya Elluri and Karuna Pande Joshi
Information Systems Department
University of Maryland Baltimore County
Baltimore, MD, USA, 21250
lelluri1@umbc.edu, karuna.joshi@umbc.edu

Abstract— **The rollout of European Union's General Data Protection Regulation (EU GDPR) will have a far-reaching effect on Cloud data privacy and compliance for both the Cloud Service Providers (Data Providers) and the Consumers (Data Consumers). GDPR mandates that organizations collecting and processing information related to EU citizens adhere to its articles irrespective of where they are located or where the data is stored. This regulation is currently available only in the textual format and so requires significant manual effort to ensure its compliance. We have developed a semantically rich Ontology (or knowledge graph) to represent the rules and regulations mandated for both the cloud data consumers and providers by EU GDPR. In the Ontology, we have identified the different roles and their corresponding obligations under the GDPR articles. This knowledge graph, that is available in public domain, is machine processable and will help in automating EU GDPR regulation compliance.**

Keywords: Data Protection; Ontology; General Data Protection Regulation; Organizations.

I. INTRODUCTION AND RELATED WORK

European Union will be rolling out an updated version of their 1998 data protection law [4] on May 25th, 2018. This data protection directive is known as General Data Protection Regulation (GDPR) [6]. As this regulation is currently available only in the textual format, it will require significant human and time effort to adhere to it. We have created a semantically rich policy-based knowledge representation of the GDPR regulation and present it in this paper. We used Semantic Web's Web Ontology Language (OWL) [3] to create this knowledge graph. We have explained each article which the cloud consumer (consumer in the GDPR) or cloud consumer (provider in GDPR) is obligated to comply with.

Pandit et. al. has proposed an ontology for GDPR [5], but they have not included detailed policy rules. In our knowledge graph we have classified the GDPR rules as obligations for consumers and providers. We also included the corresponding Cloud Security Alliance (CSA) [2][7] controls for these obligations.

II. APPROACH

We reviewed the GDPR regulation documents [1][4][6] and identified that out of the total 99 articles, only the following articles affect cloud service providers and consumers.

A. Cloud Consumer Obligations

The consumer is mainly obligated for following GDPR rules:

1. Article 5: Processing of personal data
Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject. Data is collected for a legitimate purpose and should not be processed in a manner that is incompatible for the purpose. CSA Controls: WWP-1.1, WWP-1.2, WWP-1.3 [2]

2. Article 24: Responsibly of Consumer
Demonstrates that the consumer should be responsible for implementing any technical or organizational measures which are needed for GDPR compliance. CSA Controls: DCA-1.1, DCA-1.2, REC-2.1, REC-2.5 [2]

3. Article 25: Data Protection by Design and by Default
It requires the organization to collect, store or process the data only for the required purposes by implementing techniques like pseudonymizing and data minimization. CSA Controls: WWP-1.4, REC 1.7 [2]

4. Article 26: Joint Consumers
In case of more than one consumer, this article expects all of them to be GDPR compliant. CSA Controls: CAR-1.3, REC-1.2 [2]

5. Article 27: Representatives of Consumers or Providers not established in Union
It is important to appoint a representative who is natural or legal person established in EU if the consumer or provider are located outside EU. CSA Controls: CAR-1.2, REC-1.2 [2]

6. Article 34: Communication of Personal data breach
It is required to notify the Data Subjects in clear and plain language about the data breach that might affect their "rights and freedoms". CSA Controls: PDB-1.1, PDB-1.2, PDB-1.4, PDB-1.6, PDB-1.7 [2]

B. Cloud Provider Obligations

The provider is mainly obligated for following GDPR rules:

1. Article 28 (2-4) (10): Responsibility of Processor
The provider should insist the confidentiality obligations and abide by the rules in appointing sub-providers. CSA Controls: WWP-3.2, WWP-3.3, WWP-3.4, WWP-5.1, WWP-5.2, WWP-5.3, WWP-5.4, WWP-5.5 [2]

2. Article 29: Processing under the consumer authority
The provider should process data as per the instructions provided by the consumer unless if there are any requests by Union or Member State law. CSA Controls: WWP-1.14 [2]

3. Article 37: Designation of Data Protection Officer
It is suggested to hire a Data Protection Officer in case if it involves continuous monitoring of data subject on a large scale. Also, tells that DPO must be hired based on expert understanding of privacy laws in practice. CSA Controls: REC-2.2 [2]

4. Article 44: General Principles for Transfer
Obligations regarding cross-border transfers will be applied to the data providers. CSA Controls: WWP-5.2, REC 2.4, DTR-1-1, DTR-1-2 [2]

C. *Common obligations for Cloud Consumer and Provider*

The common obligations are listed in Table 1.

Obligation	GDPR	CSA Controls
Territorial Scope	Article 3(1) [4][6]	DCA-1.2, DCA-1.3 [2]
Common Responsiblities	Article 28(1) [4][6]	WWP-1.15, RRD-3.1, RRD-4.1, RRD-4.2, CPC-1.1, CPC-1.2 [2]
Records of Processing Activities	Article 30 [4][6]	WWP-2.1, DCA-1.4, MON-1.1 [5]
Cooperation with the Supervisory Authority	Article 31 [4][6]	WWP-5.7, PDB-1.6 [2]
Processing Security	Article 32 [4][6]	SEC-1.2, MON-1.1, CAR-1.5 [2]
Data Breach Notification	Article 33 [4][6]	PDB-1.1, PDB-1.2, PDB-1.3, PDB-1.4, PDB-1.5 [2]
Right to compensation and liability	Article 82 [4][6]	SEC-1.1 [2]

TABLE 1: CONSUMER AND PROVIDER COMMON OBLIGATIONS

III. ONTOLOGY

We have developed the ontology (or knowledge graph) in OWL language using the Protégé 5 tool [8]. To develop the ontology, we have used the combination of top down and bottom up approach and incorporated these main classes: Rules/Articles that are Consumer's Obligations

- Rules/Articles that are Provider's Obligations
- Common obligations for consumer and provider
- Cloud Security Alliance (CSA) standard controls

Figure 1 illustrates the high-level classes and relationships for the Cloud GDPR ontology. Figure 2 lists all the subclasses under the main classes. This Ontology is available in public domain at [9].

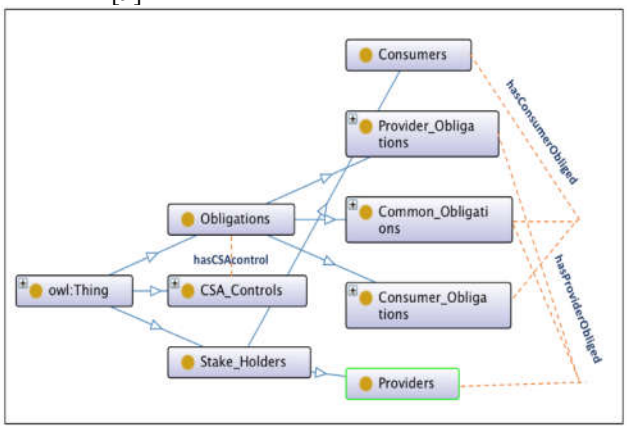

Figure 1: knowledge graph GDPR Obligations Vs CSA Controls

VI. CONCLUSION

In this work we have developed an ontology to represent the rules embedded in GDPR that affect Cloud data. We have identified the obligations of cloud data consumer and provider. We have also studied the CSA code of conduct controls and associated GDPR articles with the CSA controls in our ontology. Cloud consumers or providers can use this ontology to automate compliance with GDPR.

As part of our future work, we will be expanding the knowledge graph by associating various country obligations with standard CSA controls. With that end users can use this knowledge graph to determine all the obligations while processing cloud data.

Figure 2: Sub Classes for GDPR Obligations Vs CSA Controls

REFERENCES

[1] What the GDPR means for businesses. (2016, June 29). Retrieved March03,2018,https://www.sciencedirect.com/science/article/pii/S1353485816300563

[2] GDPR Resource Center. (n.d.). Retrieved March 07, 2018, from https://gdpr.cloudsecurityalliance.org/

[3] OWL full reference - D. McGuinness, F. Van Harmelen, et al., OWL web ontology language overview, W3C recommendation, World Wide Web Consortium, 2004.Cloud Security Alliance (CSA): Security guidance for critical areas of focus in cloud computing, v3.0 (2011). http://www.cloudsecurityalliance.org/guidance/

[4] Information Commissioner's Office: Guidance for Companies on the Use of Cloud Computing, v1.1 (2012). http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

[5] Pandit HJ, Fatema K, O'Sullivan D, Lewis D. GDPRtEXT-GDPR as a Linked Data Resource.

[6] Additional Resources about the GDPR. (n.d.). Retrieved March 07, 2018, from https://www.eugdpr.org/more-resources-1.html

[7] "WHY GDPR?" Europrivacy, europrivacy.info/2016/04/21/why-gdpr/. A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud SecurityandCompliance,"2015http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7214167&isnumber=7212169

[8] Musen, M.A. The Protégé project: A look back and a look forward. AI Matters. Association of Computing Machinery Specific Interest Group in Artificial Intelligence, 1(4)

[9] https://ebiquity.umbc.edu/resource/html/id/377/Ontology-for-EU-s-General-Data-Protection-Regulation-GDPR