Using an enterprise architecture model for GDPR compliance principles

Gaëlle Blanco-Lainé, Jean-Sébastien Sottet, Sophie Dupuy-Chessa

Using an enterprise architecture model for GDPR compliance principles

Gaëlle Blanco-Lainé[1], Jean-Sébastien Sottet[2], and Sophie Dupuy-Chessa[3]

[1] Univ. Grenoble Alpes, IUT2, 38000 Grenoble, FRANCE
Firstname.Lastname@univ-grenoble-alpes.fr
[2] LIST, 5, Avenue des Hauts-Fourneaux, L-4362 Esch-Sur-Alzette, LUXEMBOURG
Firstname.Lastname@list.lu
[3] Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG, 38000 Grenoble, FRANCE
Firstname.Lastname@univ-grenoble-alpes.fr

Abstract. Nowadays, all enterprises must take into account the legal frameworks at all levels of their organization. Over the past two years, the focus has been on the GDPR. This regulation on data and their processing activities impacts on the vision of the enterprise information system. In order to identify these impacts, it is necessary to define an approach to conciliate regulatory and business points of view. Our proposal is to use an enterprise architecture modeling approach to integrate regulatory concerns. This article describes a high-level Archimate model for implementing a GDPR compliance approach.

Key words: GDPR, architecture enterprise, regulation and compliance, privacy, model

1 Introduction

The legal framework is a major constraint for all enterprises, notably when dealing with an increasing number of legal regulations or when their complexity raises, e.g., in the financial sector [1]. Our work partially addresses this issue by dealing with the understanding of the new regulations and their consequences on the enterprise architecture. It promotes the use of models, notably Enterprise Architecture Models (EAM) to support enterprises with their obligation to regulatory compliance. In regard to this purpose, we have chosen to work on the new European regulations on the processing of personal data: the General Data Protection Regulation (GDPR) [2].

The effective date of the GDPR in May 2018 has fundamentally changed the way companies must collect and process personal data. They are now subject to an ongoing, proactive and continuous obligation to comply with the rules set out in the GDPR. Being and remaining compliant with the GDPR is currently a major issue for organizations worldwide. The problem relies on understanding legal requirements which is generally time-consuming and cumbersome [3]. Without the assistance of data protection law experts, the operationalization of the GDPR can be jeopardized, especially for small- and medium-sized organizations. To address this issue, we suggest that a legal expert helps at defining

a common model conciliating the legal and business approaches. As the GDPR constrains activities in terms of data and their processing, it can impact the information system at all levels: from the strategic level (to avoid sanctions) to the application and technological levels (to guarantee data security and privacy).

We aim at developing an reference architecture that depicts the principles of the GDPR so that it can be reused by enterprises with little legal knowledge. Our model highlights the links between the principles and the obligations supported by the regulation .It is implemented in an ArchiMate model, constituting a fragment that can be reused, by any organization for GDPR compliance.

The paper is organized as follow: first we describe related work about modelling the GDPR. Second, we introduce our approach: proposing an EAM for describing and explaining the GDPR. Third, we detail the GDPR model.

2 Related Work

With the goal of achieving compliance to the GDPR, [3] suggests that researchers and practitioners have investigated three main approaches: compliance checklists and assessment toolkits, operationalizing the GDPR with some specific data protection techniques and modeling of the regulation and its requirements.

The first approach has been developed by public agencies and private companies to support organizations in checking their compliance to the GDPR. Public agencies propose some guides for understanding the GDPR and its impact for organizations and citizen. Some of them [4] also make some self-assessment checklists. Private companies, like Microsoft [5], have provided their own toolkits to assess measures for protecting personal data. These assessment checklists and toolkits are good diagnostic tools as they can be useful to identify large gaps in compliance. However, they are not steering tools that provide concrete suggestions, particularly by taking the organizational aspects into account.

The second approach proposes some concrete data protection techniques, focusing then on a limited number of the GDPR concerns. For instance, Ayala-Rivera and Pasquale [3] define privacy controls inside system requirements, to ensure compliance to GDPR. Nevertheless they do not provide crucial legal requirements like the need for establishing a consent or a record of processing activities. Agostinelli et al. [6] propose a set of patterns for ensuring compliance of BPMN processes and fragmenting the GDPR principles for a better comprehension. However, the article focuses only on the obligations of the data controller and thus not necessarily provides rational and assistance to the overall GDPR management. Colesky et al. [7] also proposes a set of strategies and tactics to operate privacy protection. Although these works illustrate the usefulness of providing concrete suggestions for GDPR compliance, they do not provide a view of the GDPR impact on the enterprise architecture.

The last approach suggests to model the regulation concepts to achieve GDPR compliance. Some of these works rely on ontologies, using a well-known method for law modeling like [8]. This work consists of a domain ontology describing the basic elements that are required by the GDPR. A second step is

to provide a set of rules [9] to ensure compliance and to identify the gap to be compliant, e.g., [10]. Following the ontological approach, [11] proposes a framework for a generic compliance tool (i.e. compliance to any legal model) that they apply to the GDPR. However the framework relies on questions that can be ambiguous, leading to an inappropriate assessment. Moreover, if an ontology-based approach is interesting to reason on a regulation, it does not provide an organizational view of the GDPR.

Another approach, similar to ontologies, is based on a semi-formal domain model. [12] proposes a preliminary model describing the concepts of the GDPR. It scopes the domain of discourse, by depicting the kind of data (i.e. the different personal data kinds) and processes to be considered. However it needs to be completed with other models to provide some concrete help. With such goal, the work described in [13] proposes a generic conceptual model for GDPR and a global approach based on it to check compliance. By focusing on softwares, it does not provide a global view of the impact of the GDPR on the organization.

Related work presents interesting approaches to provide guidance in checking compliance and in understanding the impact of the GDPR. Nevertheless, none of them proposes a global vision of the GDPR effects at all the levels of an organization. With such goal, we propose to model the GDPR regulation at the different levels of an enterprise architecture.

3 Towards a GDPR architecture

3.1 Introduction to GDPR

In an attempt to clarify the area of work, it is important to review some elements of the GDPR. Following the European directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the GDPR reaffirms the obligation of enterprises to respect a set of obligations aimed at protecting personal data: prior consent collection, data minimisation, security, etc.... These obligations, described in 7 key principles (see Fig. 1) have marginally changed between the two regulations.

The GDPR removes the obligation of prior notification to the authorities (Article 18 Directive 95/46/EC) and replaces it with the obligation for companies to prove at any time at the request of the supervisory authority that their processes comply with the regulations. This is the principle of accountability. This paradigm shift implies a reinforced obligation for enterprises to document and monitor all their processing operations relating to personal data. To ensure compliance with all the principles and ensure regulatory compliance within accountability, the processes corresponding to each of the 7 key principles must be defined. If the obligations within the GDPR are not scheduled, the nature of the data and processes to be put in place for compliance and maintenance leads to the definition of a logical order of implementation (see Fig. 6).

Moreover we introduce some definitions to facilitate the understanding of the rest of the paper: **data controller**, according to article 4(7) is: “the natural or

legal person,[...], alone or jointly with others, determines the purposes and means of the processing of personal data". A **data subject** is natural person whom the data collection will identify directly or indirectly. The **Consent** means any informed agreement to the processing of personal data (article 11 GDPR).

3.2 Global approach

Our approach aims at providing a global viewpoint of the GDPR in terms of the rights and requirements it conveys. It has been realized by a legal expert for interpreting and explaining the GDPR and a collaborative modeling work between the legal expert and computer scientists.

To provide a global viewpoint, EAM constitutes an interesting solution. It offers different perspectives, including in particular a regulative perspective [14] which is naturally of interest to our work. By nature, EAM embeds principles that can be related to regulation aspects, e.g, recommendations, requirements, impositions, etc. As a result, we depict the GDPR regulation as a part of an enterprise architecture. This idea is also conveyed in a reference model for regulation [15] and in reference organization/enterprise models [16]. The GDPR regulation and its objectives for compliance cover only a part of enterprise architecture concerns: so we will define some architecture fragments [17]. But the layers beyond the business one are specific to an implementation of the regulatory compliance solution; we did not study them.

We selected the ArchiMate language as it fits with our modelling goals: having a support for modelling regulation as architecture; being compatible and potential partially incorporated within an actual enterprise architecture model.

3.3 Domain and Goal Models

First of all, understanding a regulation implies understating its underlying vocabulary and semantics [12, 8], i.e. establishing a domain model or an ontology. The legal text defines more or less explicitly, the relevant concepts and their relationship. To complete this initial model, we also looked at cases, jurisprudence which may refine the concepts of the law. The domain model notably defines, what are the type of personal data (e.g., marital status, genetic data, etc.) and the kind of processing activities (e.g., profiling, data transfer, etc.).

In a second time, we analyze the underlying principles of the regulation. They can be modeled as goals [18]. Those goals, also provide a rationale (i.e. belonging to the motivation layer) and the fundamental organization for the regulation architecture we provide. This approach requires a complete study of the regulation: each regulation contains explicit rights, principles which can then be translated into (regulatory) goals. Each goal is then refined into outcomes and requirements. Each requirement helps in defining the necessary measures to be put in place for compliance. It can be either a rule or a process or an organizational structure. To generalize this, we use the concept of business service.

3.4 Services and processes

Business services define the entry points of actions, sub-systems, processes to be performed by an enterprise to be compliant with the regulation. They represent answers to the previously defined regulatory requirements. They can be grouped by important core regulatory functions, such as processing activities and personal data maintenance. Contrary to [18] which expresses GDPR links between goals, we define the dependency relationship between services: the legal principles, and so goals, are to be considered as self-contained elements. But, the business implementation may require information from another service. As a result, we have to define an orchestration between the services that express the regulation.

Then we study each regulatory service and we define their behavior using a high business processes description. Each service and their process implementation manipulate the related domain elements.

3.5 Implementation in organizations

By having the regulation formalized as an architectural fragment, we aim at simplifying its integration into an existing architecture or one in the process of being defined (following the principle of compliance by design). We want to ensure that a process (application and infrastructures) is in place in order to support the corresponding business service. An Enterprise Architect has to bridge this fragment to its specific implementation in the enterprise. We try to be as much generic as possible regarding enterprises. As a consequence, we cannot go deeper into the applications and technical layers. For instance, the data retention period defined in the GDPR implies many different implementations of deletion when the retention period expires as it depends on the data support (paper, usb-key, internal information system, etc.).

4 Modeling GDPR in ArchiMate

4.1 GDPR principles: Motivation View

As proposed in Section 3, we first need to understand the GDPR domain model and goals. As domain models have already been proposed [12, 13], we focus here on regulatory goals.

We define an ArchiMate motivation view for the regulation (Fig. 1) which helps to clarify the regulatory obligations with regard to the key principles of the GDPR, set out in article 5 of the regulation.

First, the GDPR analysis highlights two important identifiable areas in terms of regulatory obligations, compliance and accountability associated with their control elements, Privacy Impact Assessment (PIA) and the record of processing activities (see Section 4.4). These two obligations are represented as drivers in the ArchiMate model. Then drivers give rise to goals that correspond to the 7 key principles for the protection of personal data as they constrain the activities of enterprises in terms of data and processing:

1. **Provide transparency on information about personal data usage** corresponding to the principle of transparency.
2. **Obtain consent** corresponding to the principle of free and informed data collect and usage.
3. **Ensure personal data accuracy** corresponding to the principle of data accuracy, requiring enterprises to provide procedures for updating data.
4. **Restrict personal data collect** corresponding to the principle of minimization of data collection, according to which all personal data collected must strictly comply with a purpose legitimately pursued by the enterprise.
5. **Restrict personal data processing activities scope** according to which the processing on data must be directly linked to the enterprise activity.
6. **Ensure right to oblivion** corresponding to the principle of respect for the right to be forgotten.
7. **Ensure personal data security** for the data security principle.

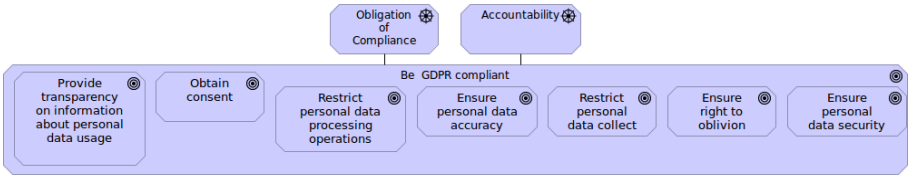

Fig. 1. GDPR Motivation View

Article 5 of the GDPR sets out the obligation to obtain the data subject's consent (goal 2, Fig. 1). It must be free and informed, which implies that collecting consent must be accompanied by sufficient information arising from the obligation of transparency.

This obligation (goal 1 in Fig. 1), described in article 13 of the GDPR, is based on the ability for the enterprise to provide data subjects with sufficiently complete information at the time of personal data collection about the enterprise, the data collected, their storage period, the processing operations to ensure the right to oblivion (goal 6). In addition, it should describe all the processing operations using personal data, the purpose of these operations, as well as the data security measures (goal 7). These data security measures are set up within the enterprise to prevent any use not in line with the stated objectives, and to ensure their confidentiality and integrity. Depending on the enterprise activity, these elements will have to be supplemented by general information on how to exercise the rights to ensure data accuracy (goal 4) or forgetting, and the possible means of recourse available for the persons concerned. The GDPR also limits the collect and processing operations (goals 5 and 3) of personal data to data and operations strictly necessary for the enterprise activities.

4.2 Requirements and Business Service View

The GDPR obligations (i.e. regulatory goals) must now be refined into outcomes and requirements as explained in Section 3. The global compliance to the GDPR (i.e. goal "be GDPR compliant" in Fig. 1) involves implicitly a prerequisite of knowledge of enterprise's processes and data as well as an identification of the GDPR concerns related to these processes and data. So as outcome, a knowledge cartography (i.e, an annotated model of the enterprise information system) about the personal data and processing operation needs to be established. This cartography will then be used to reach most of the goals.

From requirements, four functional groups are defined. They represent the core GDPR functions: processing operations and personal data maintenance, consent management, data retention management, data security management.

Processing operations and personal data maintenance One implicit claim of the GDPR is to be able to identify which data and processing operations are affected by the GDPR. Data can be of different kinds of personal (e.g. civil status, location data) and particular data (e.g. racial backgrounds, political opinions). As shown in Fig. 2, the requirement *Analyse personal data and processing operations regarding GDPR* comes directly from the overall goal *Be GDPR compliant*. To perform this analysis, a review of the enterprise processing operations (collection, profiling, archiving...) on personal data (depicted by the two requirements *Realize processing operations review* and *Realize personal data review* is necessary. From this review, we obtain a cartography of enterprise data and processing activities related to GDPR. This cartography must be kept up-to-date, giving rise to the *update processing operations* and *update data collection operations* requirements. As a result two business services are needed to realize these operations: one for defining the enterprise cartography (of data and processes) and finding out what part of the enterprise system is impacted by the GDPR; and a second one for keeping the cartography related to GDPR up-to-date.

Consent Management is a central element of the GDPR regulation[1]. It determines the lawfulness of the processing operations envisaged by the data controller. As shown in Fig. 3, it contains the following requirements :

- *define a consent form* that will inform the data subject about his/her collected personal data, the processing operations that the enterprise will realize, the security means put in place. It contains all the legal information.
- *provide accessible information*: the form should be clear, understandable by the enterprise data subjects.
- *update the consent form*: the form should evolve as the enterprise evolve (information system, activities, providers, etc.) and as the regulation evolves.
- *provide a service for collecting the consent*: it corresponds to the collect of consents from data subjects.

[1] the consent itself is also seen as a deliverable, see Section 4.4

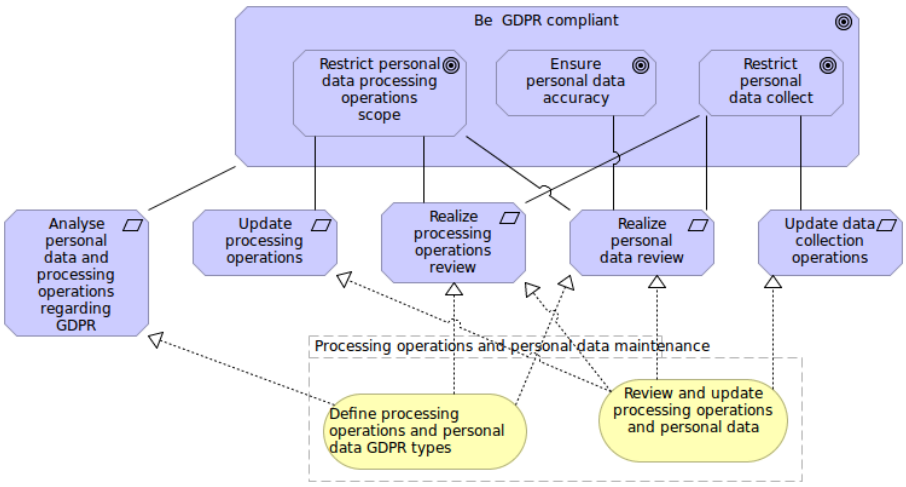

Fig. 2. Requirements for processing operations and data maintenance

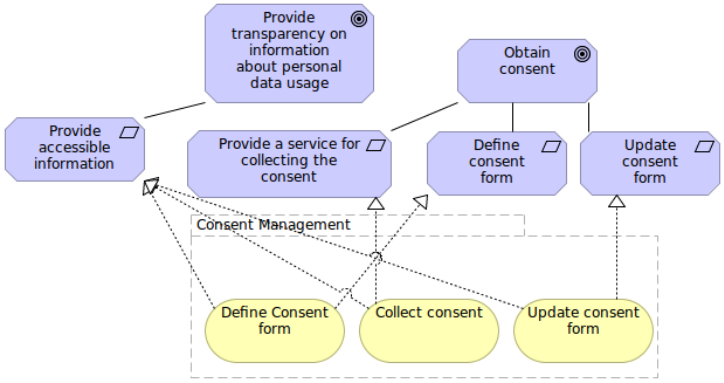

Fig. 3. Requirements and Services for Consent Management

These 4 requirements are implemented in 3 business services that will be detailed in Section 4.3. Two are related to the establishment and the update of the consent form. One is the service responsible of getting the consent information from the data subject.

Data retention management Right to oblivion is a crucial right, that is historically present in national laws. Article 5.1.e of the GDPR states that "*Personal data shall be kept in a form which permits the identification of data subjects for no longer than necessary for the purposes for which the personal data are processed*". This article gives rise to 2 requirements (Fig. 4):

– *Define personal data retention*: data retention may be limited in time regarding by legislation or by enterprise activities. A process should be put in place

to ensure that the retention time is set according to the enterprise activity or to some existing legal limitation periods.
– *Delete data impacted by the right to oblivion*: personal data must be deleted after a user request or after the expiration of the retention period. Then it should be removed from the active system but it can be stored as archive.

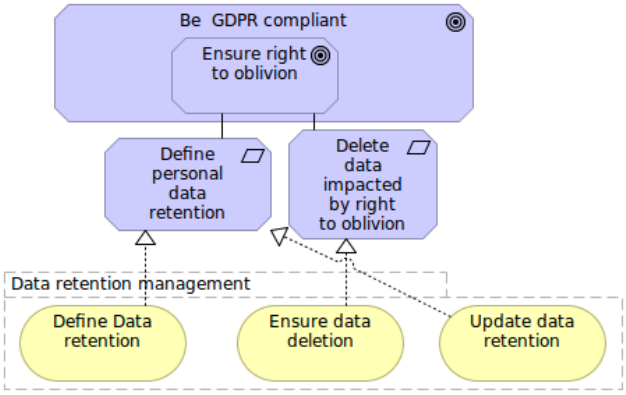

Fig. 4. Requirements and Services for Data Retention management

The related services implementation (services in Fig. 4) should ensure that the retention period is set and updated according to the evolution of the regulation or of the information system. It should also defined all the processes of deletion, pseudonymization, anonymization of personal data according to articles 5.1.e and 89.1 of GDPR.

Personal data security management The principle of data security laid down in the 2015 European Directive has been considerably strengthened with the GDPR. Article 32.2 of the GDPR refers in particular to "*risk of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed*". So the GDPR introduces two new obligations for the controller: the impact analysis and the obligation to notify if security breaches occur. These obligations correspond to 4 requirements to ensure personal data security (Fig. 5): *Formalize a security policy*, *Identify personal data security risk*, *Define personal data security risk mitigation* and, in a lesser extend, *Secure data transmission*. Indeed they are also needed to produce a Privacy Impact Assessment (see Section 4.4) and most of them touch on the risk analysis (threats identification, impacts and mitigation).

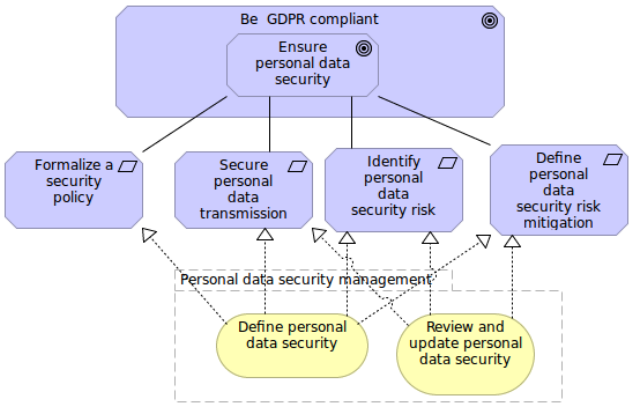

Fig. 5. Requirements and Services for Data Security Management

4.3 Details of Business Services and their orchestration

Currently, we have identified 10 business services related to the GDPR. As recommended in Section 3, these services are studied in more detail by specifying their links through an orchestration and their implementation through processes.

Business services orchestration The business services orchestration is shown in the Fig. 6. Two symmetrical paths can be followed: one when the system is put in place and another one for the system evolution. In the first case, everything starts with the identification of processing operations and data types related to the GDPR. It makes it possible the definition of both the data security and the data retention processes. It also impacts the definition of the consent form. Indeed the latter should reflect the enterprise policy (including security, retention, communication to third parties, etc) related to the previously mapped personal data and processing operations.

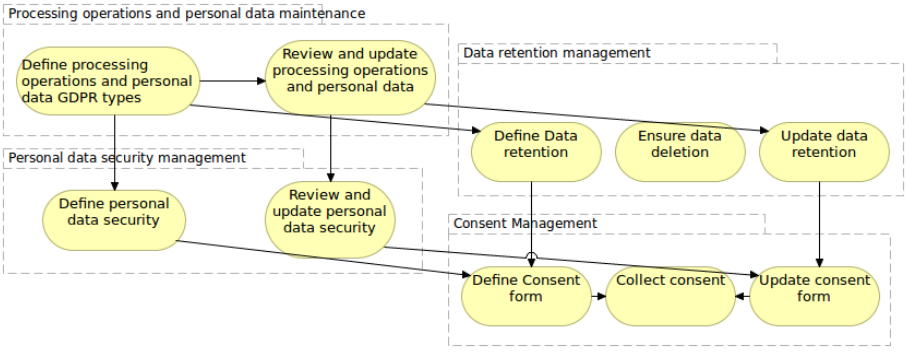

Fig. 6. Business service orchestration

For the remainder of this section, we will focus on some representative business services (one per group of Fig. 6.): *Define processing operations and personal data mapping to GDPR types*, *Define data retention*, *Define personal data security*, *Define consent form*.

As explained previously, we assume that a cartography of all the enterprise data and processing operations has been performed beforehand. For sake of clarity, the cartography is separated into two distinct business objects *Cartography of System Data* and *of System operations*, which are interleaved in practice.

Define processing operations and personal data mapping to GDPR types This service is fundamental for all other services related to GDPR. Fig 7 presents the process of tagging the system data with GDPR types like gender or genetic data. These GDPR types are provided typically by the GDPR domain analysis (e.g. like in [12] or [8]).

The first sub-process consists in checking the system regarding privacy. It answers the question: is there any personal data managed in my enterprise? Then it tags the data with the correct GDPR type (e.g. biometrics, religion, etc.). A similar activity must be realized for operations that manipulates these tagged data. Only data (to be collected) and the processes which are actually related to the enterprise activity (defined potentially in a business plan model) are retained. Finally, we restrict the collect of the personal data which are related to the previously kept processing operations. This helps in building the actual cartography as well as providing the records of processing operations.

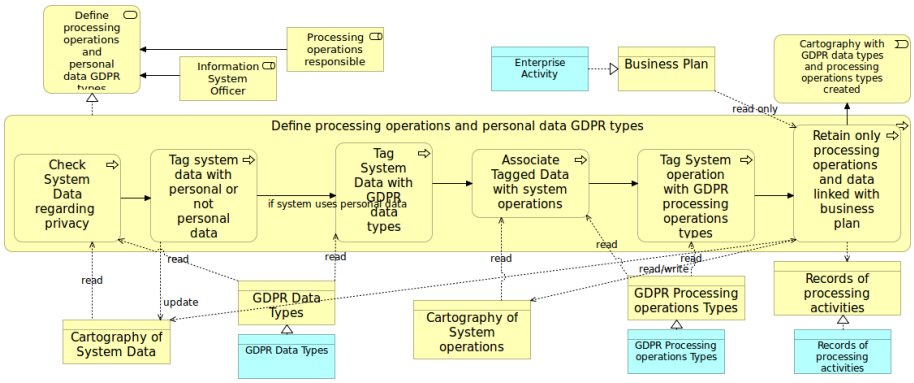

Fig. 7. Business service: mapping GDPR types on personal data and related processing operations

Define data retention This service is essential when a legal retention period exists (e.g., video monitoring should not exceed one month) or when the exploitation period finishes, or following some recommendations (e.g., the personal data about a prospect who does not answer is ideally not kept above 3

months). Such a service is thus relying on the cartography of personal data and processing operations. It starts by *Getting personal data* (Fig. 8). Then, a retention period is assigned, either according to a legal regime or according to the enterprise activity, and the cartography is updated.

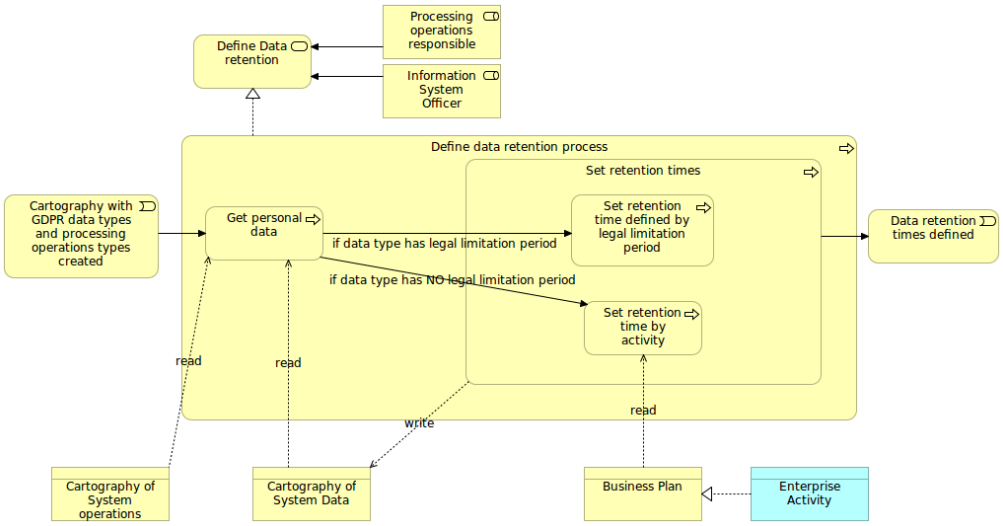

Fig. 8. Business service: data retention

Define personal data security It is aligned with the traditional risk analysis and mitigation processes: it contains part of the privacy risk assessment (i.e. the IT security aspect). As shown in Fig.9, the process consists in identifying the impacted data and processing operations, then in defining the risk - threats, impact (having three main security concerns: unauthorized deletion, modification and transmission of data). Finally, it consists in defining the security control and policy: the expected security result will be involved in the PIA, the records of processing operations deliverable and described in the consent form.

Define consent form Establishing a clear consent that informs correctly the data subject is a difficult task. The consent can only be established after all other main services were executed as it depicts the personal data, their related processing operations and their finality (in relation with the enterprise business), the retention times, the GDPR legal information and the policy necessary to ensure the data security.

4.4 Deliverable viewpoint

We finally propose a viewpoint concerning deliverables. The GDPR is based on a documentation obligation that includes two essential elements that must be

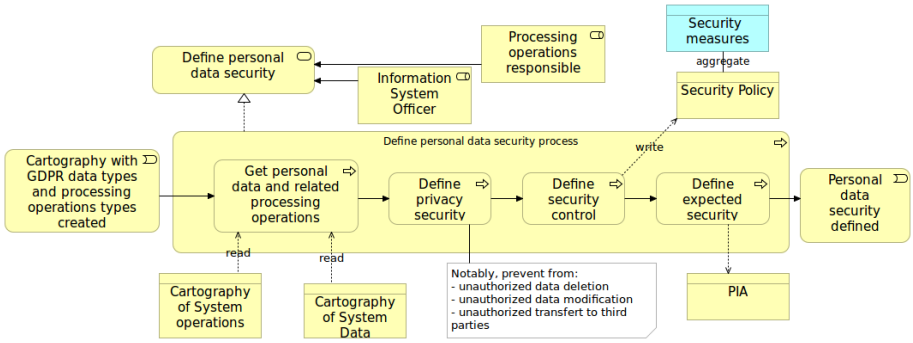

Fig. 9. Business service: define data security

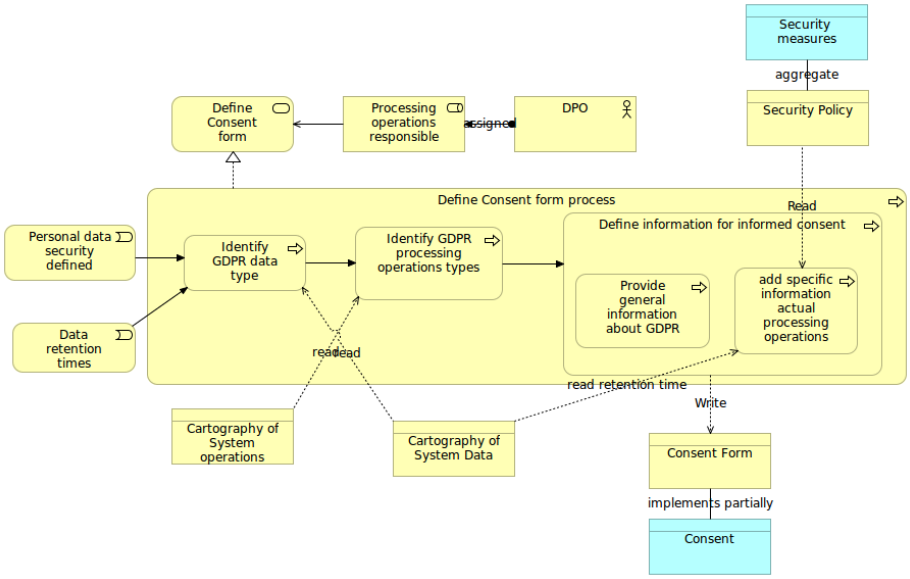

Fig. 10. Business service: define consent form

produced at the request of the supervisory authorities: the record of processing operations provided for in Article 30 and the PIA provided for in Article 35 GDPR. These mandatory deliverables are linked with the previously identified requirements (Fig. 11).

Article 30 of GDPR lists the mandatory elements to be mentioned in the records of processing operations: information identification of the controller and recipients of the data, information relating to the categories of data (types), their retention, processing activities and purpose, and a description of the technical and organizational measures put in place to guarantee the security of personal data. The records of processing operations carried out as part of accountability

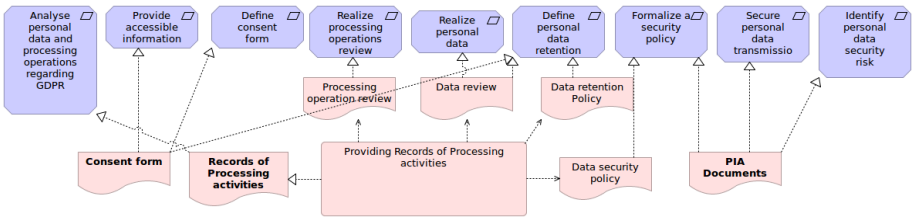

Fig. 11. Deliverable view

must be regularly updated. With such goal, four intermediate deliverables are defined to ensure continuous compliance (Fig. 11): processing operation review, data review, data retention policy and data security policy.

The PIA, 2nd mandatory element, must contain the elements of description and justification of the relevance of the envisaged processing operations. Article 35.7 of GPDR also requires the documentation of a risk analysis and management. For such requirement, standards such as ISO 27001 [19] can be useful. finally, the consent form is a central document for GDPR compliance (Fig. 11). Even if it is not explicitly cited as an obligation, it is essential for compliance to the GDPR.

5 Conclusion

This paper addresses the modelling of a given regulation (GDPR) as an EAM fragment that needs to be integrated into a more global EAM. We defined an approach for specifying a reference EAM for a given regulation: providing a motivation, services and process that an enterprise has to deal with. Moreover, an EAM fragment, depicting a regulation, helps enterprise stakeholders to understand the regulation itself, its rationale and its impacts. Notably it provides some guidance to implement the GDPR by identifying services and processes to be realized and integrated by an enterprise to be compliant. This contribution is concretized in an ArchiMate model of the GDPR.

In a future work, we will test our model on privacy by design real case studies. Then, we will try to set up a tool to help with conformance checking against existing enterprise architecture and conformance maintenance. We will address in more details some services and processes like the data transfer to third parties (notably outside the GDPR zone), the data migration right and notification of security breaches. Finally we also want to generalize the approach to many regulations and define its generic foundations.

References

1. Gozman, D., Currie, W.: Managing governance, risk, and compliance for post-crisis regulatory change: A model of is capabilities for financial organizations. In: 2015

48th Hawaii International Conference on System Sciences, IEEE (2015) 4661–4670
2. European Commission: General Data Protection Regulation (2018) https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules.
3. Ayala-Rivera, V., Pasquale, L.: The grace period has ended: An approach to operationalize GDPR requirements. In: 2018 IEEE 26th International Requirements Engineering Conference (RE), IEEE (2018) 136–146
4. Data Protection Commission - Ireland: Self-assessment checklist (2019) https://www.dataprotection.ie/en/organisations/self-assessment-checklist.
5. Microsoft: GDPR assessment: (2017) https://assessment.microsoft.com/gdpr-compliance/compliance-risk-results-133MC-2218RO.html.
6. Agostinelli, S., Maggi, F.M., Marrella, A., Sapio, F.: Achieving GDPR compliance of BPMN process models. In: International Conference on Advanced Information Systems Engineering, Springer (2019) 10–22
7. Colesky, M., Hoepman, J.H., Hillen, C.: A critical analysis of privacy design strategies. In: 2016 IEEE Security and Privacy Workshops (SPW), IEEE (2016) 33–40
8. Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., Robaldo, L.: Legal ontology for modelling GDPR concepts and norms. In: JURIX. (2018) 91–100
9. Gordon, T.F., Governatori, G., Rotolo, A.: Rules and norms: Requirements for rule interchange languages in the legal domain. In: International Workshop on Rules and Rule Markup Languages for the Semantic Web, Springer (2009) 282–296
10. Sunkle, S., Kholkar, D., Kulkarni, V.: Explanation of proofs of regulatory (non-) compliance using semantic vocabularies. In: International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer (2015) 388–403
11. Agarwal, S., Steyskal, S., Antunovic, F., Kirrane, S.: Legislative compliance assessment: Framework, model and gdpr instantiation. In: APF 2018. (2018)
12. Tom, J., Sing, E., Matulevičius, R.: Conceptual representation of the GDPR: model and application directions. In: Conf. on Business Informatics Research. (2018)
13. Torre, D., Soltana, G., Sabetzadeh, M., Briand, L., Auffinger, Y., Goes, P.: Using models to enable compliance checking against the GDPR: An experience report. In: To appear in the proce. of the IEEE/ACM 22nd Int. Conf. on Model Driven Engineering Languages and Systems (MODELS 19), ACM/IEEE (2019)
14. Bommel, P.v., Buitenhuis, P., Hoppenbrouwers, S., Proper, E.: Architecture principles–a regulative perspective on enterprise architecture. Enterprise modelling and information systems architectures–concepts and applications (2007)
15. Cleven, A., Winter, R.: Regulatory compliance in information systems research–literature analysis and research agenda. In: Enterprise, Business-Process and Information Systems Modeling. Springer (2009) 174–186
16. Timm, F., Sandkuhl, K.: A reference enterprise architecture for holistic compliance management in the financial sector. (2018)
17. Lagerström, R., Saat, J., Franke, U., Aier, S., Ekstedt, M.: Enterprise meta modeling methods–combining a stakeholder-oriented and a causality-based approach. In: Enterprise, business-process and information systems modeling. Springer (2009)
18. Ghanavati, S., Amyot, D., Rifaut, A.: Legal goal-oriented requirement language (legal GRL) for modeling regulations. In: Proceedings of the 6th international workshop on modeling in software engineering, ACM (2014) 1–6
19. ISO: ISO/IEC 27001 - information technology security techniques information security management systems requirements. Standard, International Organization for Standardization, Geneva, CH (March 2013)