Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Architecture-based regulatory compliance argumentation

Boyan Mihaylov, Lucian Onea, Klaus Marius Hansen*

Department of Computer Science (DIKU) University of Copenhagen, Denmark

ARTICLE INFO

Article history:
Received 5 May 2015
Revised 19 April 2016
Accepted 22 April 2016
Available online 24 May 2016

Keywords:
Regulatory compliance
Software architecture
Software development

ABSTRACT

Standards and regulations are difficult to understand and map to software, which makes compliance with them challenging to argue for software products and development process. This is problematic since lack of compliance may lead to issues with security, safety, and even to economic sanctions. An increasing number of applications (for example in healthcare) are expected to have to live up to regulatory requirements in the future, which will lead to more software development projects having to deal with such requirements. We present an approach that models regulations such that compliance arguments can be made in a principled way based on architectural requirements and architectural decisions. In particular, we discuss how one can form architectural requirements which are linked to regulatory texts. We then argue for completeness and correctness of this bi-directional link. We evaluate the approach on the migration of the telemedicine platform Net4Care to the cloud, where certain regulations (for example privacy) should be concerned. The approach has the potential to support simpler compliance argumentation with the eventual promise of safer and more secure applications.

1. Introduction

Many application domains require regulatory and standards compliance in systems and software development. Examples include industrial automation, transport, and the medical domain. In industrial automation, relevant regulation includes the IEC 61508 functional safety standards (ISO/IEC, 1998-2000). In the rail domain, systems may have to live up to IEC 62278 (IEC, 2002). In the medical domain, the US Food and Drug Administration (FDA) and the European Union (EU) are examples of organizations that stipulate regulatory requirements (e.g., Code of Federal Regulations (FDR), Title 21, Part 820 (FDA, 2014) and the Medical Device Directive (European Commission, 1993)).

Healthcare and the medical domain are particularly pertinent to this article in that applications are often both safety-critical and security-critical. Furthermore, recent technologies such as cloud computing and mobile computing are impacting this domain, stressing traditional governance mechanisms for healthcare applications. A count in the Apple App Store, e.g., showed that more than 40,000 applications existed in the category “health & fitness” (Manikas et al., 2014). In terms of safety, the FDA and the European Union (EU) regulate how applications that are medical devices should be built. In terms of security and privacy for health-related applications, the US Health Insurance Portability and Accountability (HIPAA; (United States Congress, 1996)) and the EU’s Data Protection Directive (European Union, 1995) are central regulations. While the legal status of mobile applications as medical devices is unclear, many of these are expected to be governed as medical devices (U.S. Department of Health and Human Services – Food and Drug Administration, 2013).

Not living up to relevant standards and regulations may have serious consequences. While applications may still be safe and secure if they do not live up to standards and regulations, there is risk related to not following standards and regulations. Furthermore, non-compliance with the regulations may lead to legal actions and fines. An example is the case of the genomics company “23andMe” that was forced by the FDA to stop providing personalized health data based on DNA (FDA, 2013). Moreover, breaching privacy regulations can in the future lead to severe fines. EU’s new, not yet finished, privacy regulations are expected to stipulate fines up to 2% of annual revenue for enterprises violating privacy regulations (European Commission, 2012b).

In this sense regulatory compliance is important, but it is challenging to integrate it into software development. Software engineers, when designing new systems, must be able to argue and communicate how these systems relate to law. Firstly, it is difficult to understand regulations and their implications for the requirements of an application. From a developer’s perspective, it is challenging to interpret and define system requirements given regulatory texts. Such texts contain qualified phrases full of

* Corresponding author.
E-mail addresses: xfl682@alumni.ku.dk (B. Mihaylov), zpm615@alumni.ku.dk (L. Onea), klausmh@di.ku.dk, klausmh@diku.dk (K. Marius Hansen).

http://dx.doi.org/10.1016/j.jss.2016.04.057
0164-1212/© 2016 Published by Elsevier Inc.

ambiguities and large numbers of references to other sections of the same document or different ones (Kiyavitskaya et al., 2007). Moreover, if engineers misinterpret these texts, for example by overlooking a condition in a regulatory rule, incorrect rights or obligations may be related to wrong stakeholders. The risk of such misinterpretations increases with the interoperation of multiple systems (Breaux et al., 2006). Secondly, compliance argumentation is typically global and is hard to reconcile with modular architectures such as service-oriented architectures, product lines, and ecosystems. Thirdly, integrating arguments for compliance with iterative, incremental, or agile processes is hard due to the complexity of making these arguments.

This paper addresses the first issue, but also lays a foundation for addressing the remaining two by making the following contributions:

- We introduce an approach for arguing about regulation compliance based on architectural requirements and architectural decisions. The approach employs “Semantic Parameterization” for modeling regulations and the “Goal Structuring Notation” for arguing compliance.
- We demonstrate the application of the approach by applying it to the case of data protection and privacy in healthcare through the evaluation of a cloud migration of a telemedicine platform, Net4Care. Because the platform is European (Danish), we focus particularly on the relevant European (Danish) regulations.

The remaining part of this paper is structured as follows. First, we provide background on (privacy) regulations, Semantic Parameterization, and the Goal Structuring Notation (Section 2). Next, we outline our approach to architecture-based regulatory compliance argumentation (Section 3) and apply it to the Net4Care case (Section 4). Finally, we discuss related work (Section 5) and draw our conclusions (Section 6).

2. Background

Several regulations related to data protection, healthcare, and cloud computing are relevant to our case. We discuss these in Section 2.1. Moreover, regulations are hard to interpret and apply in software development. To aid in interpreting regulations, we present background on “Semantic Parameterization” (Section 2.2). Finally, we present background on how to relate interpreted regulation to architectural decisions (Section 2.3).

2.1. Regulations

In general, healthcare information systems store and transfer data. Providing a cloud computing solution for such a system points to specific security and privacy issues. The biggest questions that should be raised are: “Where is my data being stored?” and “How is my data being transferred or processed?”. In this section we focus on regulations about data protection and privacy in the European Union and in Denmark in particular. A detailed discussion can be found in Mihaylov and Onea (2013).

2.1.1. EU regulations

A central, legal document regarding data protection is the Directive 94/46/EC of the European Parliament (European Parliament and the Council of The European Union, 1995).

As the Directive is mostly made up of principles regarding data protection, we have extracted the ones that are most relevant to our case:

Identification of personal data: Article 8 Section 7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Information presented to the data subject: This refers to information that has to be presented to the subject when collecting and processing the subject’s personal data. Article 10 describes the minimum information needed to ensure transparency to the subject: (a) the identity of the controller and his representative, if any; (b) the purposes of the processing for which the data are intended;

Right of access: Article 12 states that there should be a high level of transparency between subject and the controller. In short, the following should be provided: confirmation of data processing; recipients to which data might be disclosed; knowledge of processing logic of data; ability to rectify, erase or block data if it does not comply with the provisions of the Directive;

Confidentiality: According to Article 16,

> “Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.”

Security of processing: According to Article 17,

> “Section 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access [...]”

The regulations in the directive outline general principles about personal data protection in the EU. Largely, the principles state that security and confidentiality should be implemented according to a risk assessment of the system that handles data processing, while taking into account a certain level of transparency to the data subject regarding the subject’s personal data. In terms of data transferred between member states and countries outside the EU, the Directive states that all parts should ensure compliance with the policies stipulated in the document.

This relatively old directive was written before the breakthrough of the Internet and as a result it does not take into account how the Internet, and the laws regarding it, have evolved over the last two decades. In January 2012, a new proposal for a General Data Protection Legislation has been issued by the EU Parliament. This new regulation aims to add and enforce key concepts from the previous directive (European Commission, 2012a) such as guaranteeing easy access to one’s own data, right to be forgotten (deletion of data), explicitly given consent for processing data, ensuring a single set of rules for all member states, and clear rules for data controllers outside the EU. The proposal is expected to be approved in early 2015 and come into force two years later.

2.1.2. Danish regulations

In Denmark, data security and privacy are stipulated by the Act on Processing of Personal Data (the Act) (Datatilsynet, 2013) and the Executive Order on Security (Datatilsynet, 2011a). The former aims to stipulate the processing of personal data for individual citizens in general. It is intended to be flexible and take into consideration the use of modern technologies (Datatilsynet, 2013; 2011b). Lastly, it implements EU’s Directive on the protection of personal data (European Parliament and the Council of The European Union, 1995). On the other hand, the Executive Order on Security is intended for the processing of personal data on behalf of the public administration (Datatilsynet, 2011a). According to Chapter 16 of the Act on Processing of Personal Data, the Danish Data Protection Agency (*Datatilsynet*) is responsible for all processing operations covered in the act (Datatilsynet, 2013, Chapter 16).

When using cloud computing for storing or processing sensitive data, we should be aware of several important points, according to the Danish data privacy law – location, access, and processing. All data centers must (i) implement the necessary security mechanisms to cover the regulations in the Act on Processing of Personal Data and the Executive Order on Security. Furthermore, it is necessary (ii) that data transfer from one data center to another is done only if both states, in which the data centers are located, implement adequate security policies (EU/EEA members with privacy regulations enforced or the US under a Safe Harbor Agreement). Access to data should be logged (iii) so that it can be seen from the log history who did what. This can help law enforcement when investigating, e.g., data disclosure. Moreover, denied access attempts (iv) should also be logged and further analyzed on regular basis. This measure is necessary due to the possibility of unauthorized access to the data with the purpose of disclosing, destroying, or modifying these data. Lastly, as there can be many processors, each of them must (v) comply with the rules when working with the data and the controller must ensure these rules are obeyed. Furthermore, a contract between the controller and each processor must be signed for legislative purposes. Also, according to the healthcare law, one must have the patient's consent before disclosing treatment data to multiple parties.

Although we try to cover private data processing in different aspects of the law, we do omit some parts in order to keep the focus at the approach itself, rather than introducing more complexity. One such part is about keeping data in a structured and searchable format when dealing with cases in the public administration and the healthcare. This part is defined in the Executive Order on Public Records for Healthcare Personal (*Journalføringsbekendtgørelsen for sundhedspersonale*) (Sundhedsstyrelsen, 2013) and the Act on Public Records for Administration (*Offentlighedsloven*), (VI MARGRETHE DEN ANDEN, 2013, Section 15).

2.2. Semantic parameterization

Regulatory texts are difficult to understand and apply by people who do not have a background in the legal domain. Software engineers, when designing new systems, must be able to argue and communicate how these systems relate to regulations. In order to support this process, our compliance argumentation approach uses *Semantic Parameterization* – a mechanism for creating a model out of regulatory texts. This framework allows us to argue about the meaning of the legislation and further create new software requirements and enable the traceability from these requirements back to the regulations. It is based on the work of (Breaux and Antón, 2008) and relies on the Grounded Theory (Glaser and Strauss, 1967) to encode rules from regulations. The process contains the following general activities:

- Create definitions of stakeholders and stakeholder hierarchies
- Annotate paragraphs from regulatory texts to support understanding
- Extract rights, obligations, and constraints from the annotated paragraphs by applying extraction patterns

The general idea of this framework is to create simple rules in the form *< actor> may/must do < something> on < another thing>*. We first begin with describing a few terms used by the modeling framework (Glaser and Strauss, 1967; Breaux et al., 2006).

- A *right* is a statement about an activity that a stakeholder is permitted to engage in. The stakeholder is not obligated, but rather has the option, to perform this activity. These statements are typically expressed with the constructions *may* or *has the right to*.
  Example: Private bodies may process data.
- An *obligation* is a statement about an activity that a stakeholder is required to do. As opposed to the *right*, the stakeholder is now obligated to perform this activity. Typical expressions are *must, shall* or *should*.
  Example: Common processor must erase data.
- If a statement does not expressly obligate a stakeholder to perform an activity, it is called an *antiobligation* and is considered a *right*.
  Example: Controller shall not entitle a data subject to a new communication.
- If a statement is expressly disallowing a stakeholder to perform an activity, it is called a *refrainment* and is considered an *obligation*.
  Example: A company may not disclose data to a third company.
- *Rights* and *obligations* typically impose restrictions depending on the context (on the stakeholders or on the action performed by them). These restrictions are called *constraints*.
  Example: Data which are to be processed must be adequate.

Semantic Parameterization is a mechanism that allows us to extract rights and obligations from regulatory texts in "Restricted Natural Language Statements" in order to describe discrete activities (Breaux et al., 2006). It was developed using Grounded Theory, in which the theory that is systematically obtained from a dataset is valid for that dataset (Breaux et al., 2006). We apply four basic extraction patterns to restate legislative texts as rights and obligations:

- The *basic activity pattern* identifies sentences where a subject performs an action on an object (Breaux and Antón, 2008). In order to distinguish between a right and an obligation, one uses modality (e.g., may or must). Constraints rarely have modality.
- The *purpose pattern* identifies "the high-level goal or reason for performing an action" (Breaux and Antón, 2008). This includes sentences such as "... to do something ..." or "... in order to do something ...".
- The *pattern to distinguish nouns by verb phrases* identifies additional constraints. This pattern is usually applied to subsentences in the form who/that/which + a verb.
- The *rule pattern* identifies pre- and postconditions as constraints (Breaux and Antón, 2008). This includes sentences with conditional words and phrases, e.g., if, unless, upon, provided that.

The regulatory documents have been processed manually, where we have gradually applied these patterns while reading a given text. Each right, obligation, and constraint is given a unique identifier (ID) used for reference. Every right or obligation should be expressed in the simple form and therefore we have applied the *basic activity pattern*, which ensures that we have exactly one subject, one verb, and one object. The same applies to the constraints, though we have not split all of them for the sake of simplicity. Furthermore, each right or obligation may contain one or more constraints expressed as logical conjunctions and disjunctions (e.g., $C1 \vee (C2 \wedge C3)$).

2.3. The goal structuring notation

To argue that a software architecture that fulfills architectural requirements is compliant with regulations, we will use a formal notation, called the *Goal Structuring Notation* (GSN). This notation supports the development of arguments for a "goal" (hence the name) and enables different solutions to be attached to it in order to argue for this goal. An argument can be defined as "a connected series of claims intended to establish an overall claim" (Attwood et al., 2011). In the process of persuading others of the truth of a claim, some supportive claims will be necessary, and thus creating

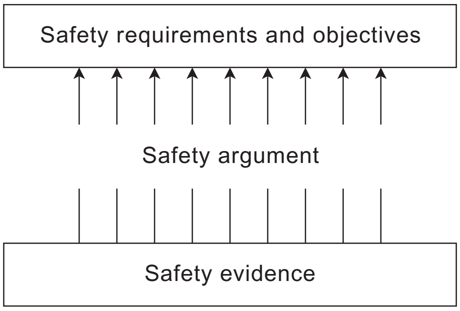

Fig. 1. Safety case components (requirements, argument, and evidence) and their relations. Adapted from (Kelly and Weaver, 2004).

a hierarchy of claims, by which an argument is established. GSN represents the claims as *goals* and the corresponding evidence as *solutions*.

Arguments developed and presented using GSN "can help provide assurance of critical properties of systems, services or organizations" (Attwood et al., 2011). The standard has mainly been used to provide safety assurance and therefore most of the organizations that have contributed to the standard deal with safety. The concept of a safety case is adopted and used across many industries, e.g., defense, aerospace, and railways. A safety case has three general components – requirements, argument, and evidence (Kelly and Weaver, 2004), shown in Fig. 1.

The argument is the glue between the requirements and the evidence. It is as important as the evidence itself: if we do not support an argument by at least one piece of evidence, then the argument becomes empty and unconvincing. On the other hand, if we have an evidence without an argument, we miss the details about how exactly the evidence fulfills the requirements.

Although GSN has primarily been used to argue safety cases, we can also use it to argue for regulation compliance: the goal in our case is to demonstrate that a software architecture (described via architectural decisions and architectural requirements) complies with regulations and the arguments of GSN can link this goal to solutions providing architectural decisions as evidence.

2.3.1. Notation overview

The notation employs a set of elements to show whether a claim holds true or not. Every element has a unique ID and a special shape. The following explains the basic elements used by the notation (Attwood et al., 2011). Examples are shown in Fig. 2.

Goal represents a claim. It can be supported by sub-goals, which means that when all its sub-goals hold true, then the goal itself holds. It is represented as a rectangle. The ID usually starts with "G".

Strategy provides further details about how a goal will be established. It is represented as a parallelogram. The ID usually starts with "S".

Solution contains the actual means by which a goal will be established. It is represented as a circle. The ID usually starts with "Sn".

Assumption provides an assumption about a branch of goals (or just one goal). If this assumption holds, then reasoning is valid for the branch. It is represented as an ellipse. The ID usually starts with "A".

Justification is used to justify a particular goal or argument strategy in order to provide extra explanation as to why the goal or strategy is considered acceptable. This applies only to the goal or strategy and not to their children. It is represented as an ellipse. The ID usually starts with "J".

Context gives evidence about the context, in which the goal is situated. It is represented as a rectangle with rounded corners. The ID usually starts with "C".

A GSN model may further contain "modules". A module may consist of all the elements mentioned above. Furthermore, an "away goal" can model a goal that is part of another module. In addition to the standard elements, there are two important relations used to connect them (Attwood et al., 2011).

InContextOf is used to declare a contextual belonging. It is represented as lines with hollow arrowheads.

SupportedBy is used to indicate inferential or evidence-based relationships between elements. It is represented by lines with solid arrowhead.

3. Architecture-based regulatory compliance argumentation

Here we explain how we argue that a software architecture of an application describes a system that is compliant with regulations. Our assumptions are that a complete and correct architectural description exists and that relevant regulations have been identified. In this context, a "complete" architectural description describes the application fully and a "correct" architectural description is correctly describing the application to be built.

Given this, the steps of our approach are:

(i) Apply Semantic Parameterization to the regulatory texts to define the involved actors and extract rights, obligations, and constraints. We begin by creating stakeholder hierarchies. This will give us all involved actors and later will help us argue the application of a right or obligation to a specific actor. For example, the following definition contains a class

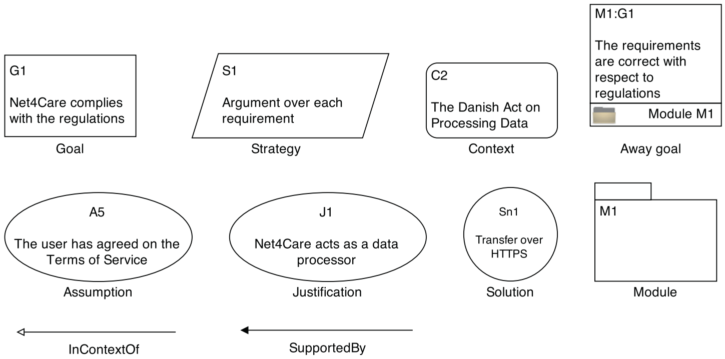
G1
Net4Care complies with the regulations
Goal
S1
Argument over each requirement
Strategy
C2
The Danish Act on Processing Data
Context
M1:G1
The requirements are correct with respect to regulations
Module M1
Away goal
A5
The user has agreed on the Terms of Service
Assumption
J1
Net4Care acts as a data processor
Justification
Sn1
Transfer over HTTPS
Solution
M1
Module
InContextOf
SupportedBy

Fig. 2. The GSN notation. Examples taken from our model arguing for the regulation compliance of a modified Net4Care. Each shape is labeled underneath with the name of the element or relation it represents.

Controller, with five subclasses – *Natural person, Legal person, Public authority, Agency*, and *Body*.

> Controller is “a natural or legal person, public authority, agency or any other body [...].”

There are many paragraphs in the regulatory document that do not explicitly state the subject. We resolve this ambiguity by using the surrounding context and in some cases we introduce a new stakeholder, based on this context. In the following excerpt we have decided to introduce a new stakeholder – *Common processor*, which is parent of *Controller*.

> “5. (2) Data **must be collected** for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes.”

The next part is to categorize the actors from our stakeholder hierarchies into “internal” and “external” actors relative to the context of the system (i.e., whether their influence to the system is from the inside or from the outside, respectively). From the previous example, a *Controller* could be defined as internal to the system since it could be part of the context of the system, whereas the *Data subject* (the one who owns the data) is an external stakeholder.

Rights, obligations, and constraints are further extracted with the help of the four patterns discussed earlier. Each right and obligation gets a unique ID so that we can reference it later. Constraints are expressed as simple sentences (see 2.2) and joined by the boolean operations AND, OR, and NOT, they define the context of each right and obligation. The following is an excerpt from a regulatory text.

> “A company may not disclose data concerning a consumer to a third company for the purpose of marketing [...]”

It defines an obligation – *A company may not disclose data*, with a subject in charge *Company* and with three constraints – *Data concerns a consumer, Data is disclosed to a third party*, and *The purpose of disclosure is marketing*. The constraints are joined by logical AND.

Rights and obligations are correspondingly categorized both into external and internal according to the actor they relate to.

(ii) Describe architecturally significant requirements of the software architecture of the application, e.g., using quality attribute scenarios (Bass et al., 2012). Annotate these requirements with related rights and obligations from step (i) – this is a manual process which involves going through each requirement and trying to identify possible rights and obligations that could affect it. The process requires that one has a good understanding of the entire system along with the extracted rights and obligations. With more complex systems this could become very time consuming and error-prone and hence require many people and many iterations.

For example, the obligation *Controller shall inform the person whether or not data are being processed* could lead to the imposition of the architectural requirement *Access to healthcare data should be logged*.

(iii) Create a GSN-based argument with the hypothesis that the application implemented as described by the software architecture complies with regulations, arguing correctness and completeness. In this step we create the actual GSN model, where we have two general claims: the requirements comply with the regulations and the regulations are encoded in the requirements. This step serves two purposes:

(a) As the process of mapping requirements with rights and obligations is done manually, it is possible to a miss a certain mapping. So this step aims to decrease the possibility of missing such a mapping.

(b) To visualize all these mappings for further argumentation and maintenance.

When creating the model, the topmost goal denotes the general compliance and it is split into two sub-goals for each part described below (it could be seen as a tree with two main branches).

(a) Correctness: requirements are correct with respect to the regulations, i.e., they are permitted by the regulations:

```
for all re : requirement do
    correct ← false
    for all r : internal right do
        if (r allows re) then
            correct ← true
        end if
    end for
    for all o : external obligations do
        if (o allows re) then
            correct ← true
        end if
    end for
end for
```

In this branch of the main tree each requirement becomes a goal, where all internal rights and external obligations that could affect this requirement are attached as context. If the scope of the requirement is very big, it could be split further into smaller ones. At the end of the each branch (the leaves) in this subtree is the solution, explaining how the requirement will be implemented (technically). The actual solution must take into consideration the context of each goal it applies to.

Let’s take a look at the following system requirement:

> *Telemedical observations shall be synchronized with the national registry.*

This becomes a sub-goal in the correctness branch of the model tree. Next we have to go through all rights and obligations and to find the relevant ones for the requirement – they become the context of the sub-goal.

(1) Obligation: *Data must be collected for specific purposes*

(2) Obligation: *Data must be processed in accordance with good practices*

When we have identified the context for our sub-goal, we can shape our solution in a way that it satisfies all constraints, i.e. it obeys the relevant rights and obligations. A possible solution in this case could be *Secure transfer of data over the network*. A solution may also indicate how the process should be lead rather than being pure technical.

(b) Completeness: requirements are complete with respect to the regulations, i.e., what the regulations stipulates is supported by requirements

```
for all or : internal obligation or external right do
    complete ← false
    for all re : requirement do
        if re supports or then
            complete ← true
        end if
    end for
end for
```

In this branch of the main tree each internal obligation or external right is represented as a goal. Justifications or assumptions could be attached to the goals if such exist in the extracted model from the Semantic Parameterization. The solutions in this sub-tree are the requirements themselves, showing the relationships with the rights and obligations.

If we take the two obligations from above, they become sub-goals in this branch of the model tree and both have the given system requirement as a solution.

(iv) Derive a conclusion based on GSN argument is the final step. It requires going through the GSN model and identifying any parts lacking support or explanation. This conclusion could (and probably should) be verified by a lawyer in a related field (e.g., software engineering and data privacy). Afterwards it could be used as a proof (along with the GSM model itself) that the system complies with the regulations.

It is important to note that our approach assumes that complete and correct architectural description exists and that relevant regulations have been identified, which may be challenging in the real world. However, for a software system that needs regulatory approval, this is essential. According to a survey by Thomson Reuters in 2015, organizations expect significant increase in the demand for regulatory compliance and the need for adjusted IT processes and systems (Thomson Reuters, 2015). Moreover, these organizations expect the cost of compliance to increase due to the increased risk and the associated fines when ineffective or no measures are taken.

In the next section we apply the approach to the Net4Care case of a telemedicine platform migration to a cloud platform.

4. Cloud migration of Net4Care

Net4Care is a software platform that is part of the open source software provided by the Danish "Society for software-based health services" (4S[1]) and is as such intended to provide the platform for a telemedicine software ecosystem (Christensen et al., 2014). The platform supports the creation of integrated telemedical applications that are based on the HL7/PHMR and IHE/XDS international healthcare standards. A working scenario could be that a developer creates a mobile application which communicates with a specific medical device, e.g., a Bluetooth-enabled armband that measures ones pulse while running. The data from the medical device is transmitted to the phone and then to the Net4Care server, which processes these data and generates corresponding clinical HL7/PHMR documents and potentially stores them in a national IHE/XDS repository. Net4Care's architecture is described in full in Net4Care (2012). The platform itself is implemented in Java, where the server-side part is based on the OSGi platform. Client libraries for Android and C# as well as a REST API are also available.

As part of the work reported in this article, we considered deploying Net4Care to a public cloud to support the goal of letting Small-and-Medium-sized Enterprises (SMEs) deploy Net4Care and use scalability mechanisms of clouds to improve performance. As part of these consideration, we made an initial analysis of Net4Care's architecture from a security and privacy point of view.

The following are particular problems with the present architecture found based on an understanding of Net4Care and regulations. In addition, resources such as the cloud computing risk assessment approach of ENISA (European Union Agency for Network and Information Security, 2009) and the advice from the Danish Agency for Digitisation (Digitaliseringsstyrelsen) on the legal framework for cloud computing (Digitaliseringsstyrelsen, 2012) could be taken into account.

- The *lack of explicit legal knowledge* leaves a burden for the person responsible with system installation. This person must have knowledge about processing of personal data. Typically these people do not have insight in the legal domain and hence they need, e.g., a lawyer to guide them.
- *Using personal identification numbers as an identifier* is not a good practice as it is considered personal data. Passing personal identification numbers from one system to another is in conflict with the regulations about transmission of personal data.
- When personal data is not needed, it *should be erased*, so it cannot be accessed anymore. This might be an issue with the current implementation, as the Net4Care cache is very simple and does not provide any clearing functionality.
- Medical data (i.e., observations) is *available to everyone*, which exposes a risk of revealing personal data to people, who should not have access to it.
- There is no *separation between healthcare professionals and patients*, so it impossible to apply restrictions to data access.
- There is no way to *track actions in the system*, which may lead to uploading or retrieving of personal data from unauthorized people. Moreover, there is no possibility of *tracking unauthorized attempts*.

At the point of this analysis, Net4Care has very basic support for privacy and healthcare regulations. This support is limited to logging of basic operations, e.g., querying and retrieving observations, though with missing details concerning authorization and authentication.

4.1. Step (i). Model regulatory requirements

We have first applied the framework to the Act on Processing of Personal Data (Datatilsynet, 2013). We have only considered the following chapters as relevant (see Section 2.1.2):

- Chapter 4 Processing of data
- Chapter 7 Transfer of personal data to third countries (without 27. (6))
- Chapter 8 Information to be given to the data subject
- Chapter 9 The data subject's right of access to data
- Chapter 10 Other rights
- Chapter 11 Security of processing
- Chapter 12 Notification of processing carried out for a public administration
- Chapter 13 Notification of processing operations carried out on behalf of a private controller
- Chapter 15 Miscellaneous provisions

The first step, as discussed above, is to create stakeholder hierarchies. Chapter 2 contains a list of definitions of expressions used in Datatilsynet (2013). The definitions of the most used stakeholders are:

Controller is "a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data".

Processor is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

Third party is "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data".

[1] http://www.4s-online.dk

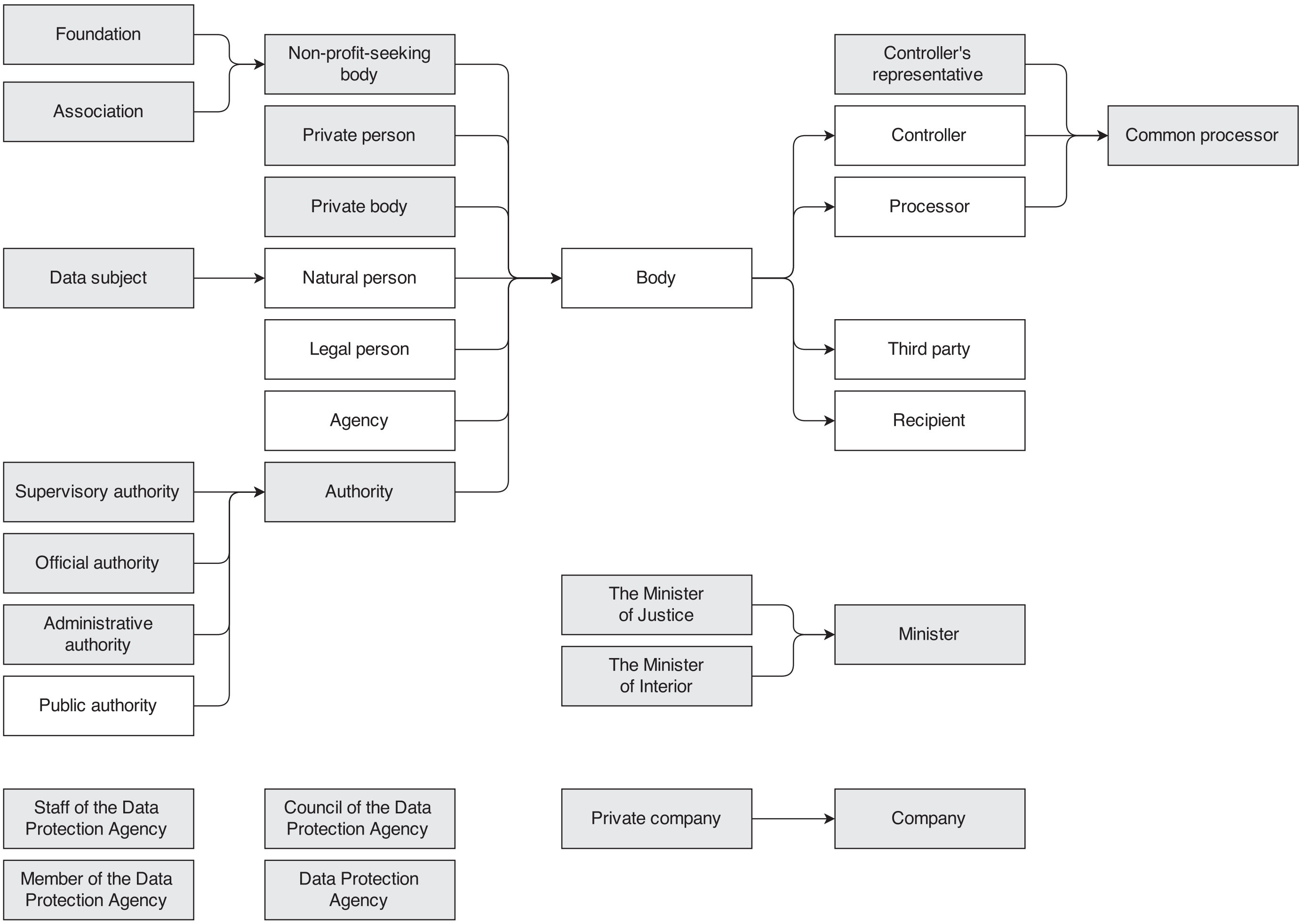

Fig. 3. Stakeholder hierarchies identified from the Danish Act on Processing of Personal Data. The white boxes represent stakeholders, which are explicitly stated in the legal text, while the gray boxes represent stakeholders that we named, but their implicit description exists already in the legal text.

Recipient is "a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not". Authorities, which may receive data in the framework of a particular inquiry, shall not be regarded as recipients.

Here, the *Controller* stakeholder, e.g., is internal to Net4Care since it is part of the context of Net4Care whereas the *Data subject* is an external stakeholder.

The first definition says that there is the class *Controller*, along with other five subclasses – *Natural person, Legal person, Public authority, Agency*, and *Body*. The same applies for the definition of a processor, a third party, and a recipient. Moreover, we can infer that the class *Body* is actually a superclass of all other classes, i.e., *Natural person, Legal person, Public authority*, and *Agency*. We have, however, additional constraints on these subclasses, which differ from each other, e.g., the subclass *Natural person* of the class *Controller* differs from the same subclass of the class *Processor* (see the underlined parts above in the definitions). The document also contains other stakeholders, which are not explicitly defined in Chapter 2, e.g., the paragraph below, which indicates that *The Minister of Justice* should also be interpreted as a stakeholder.

> "34. (2) The Minister of Justice may lay down rules for payment for communications which are given in writing by private companies, etc."

The stakeholder of the text are The Minister of Justice, The Minister of Interior, The Data Protection Agency, Supervisory authority, Administrative authority, Public authority, Data subject (a body, to whom data is related).

Unfortunately, there are many paragraphs in the document that do not explicitly state the subject. This causes ambiguity, which we resolve by using the context of the law. In some cases we have to just introduce a new stakeholder, based on the legislation text. Consider for example the following excerpt:

> "5. (2) Data **must be collected** for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes."

There is no explicit subject in this definition. In these instances we need to infer who the subject is, based on the provided definitions in Chapter 2 and the available context. In the case of section 5. (2) and others similar in the document we decided to introduce a new stakeholder – *common processor*, which can be either a controller or a processor.

Fig. 3 shows the stakeholder hierarchies that we have identified from the Danish Act on Processing of Personal Data. The stakeholders colored in gray are inferred from the document, while the rest are based on the definitions provided in Chapter 2. The relations between classes are not complete, i.e. the subclasses to a class do not describe all possible subclasses in reality, but rather those that are mentioned in the legislative text. Moreover, these subclasses are not by any means separate, e.g., the class *Private body* includes objects (in terms of object-oriented programming), which are also

Table 1
A sample list of constraints extracted from the data privacy regulations.

ID	Text	Source
C1	The data subject has given his explicit consent.	6.(1)
C2	Processing is necessary for the performance of a contract.	6.(1)
C3	The data subject is party to a contract.	6.(1)
C4	Processing is necessary in order to take steps at the request of the data subject prior to entering into a contract.	6.(1)
C5	Data concerns a consumer.	6.(2)
C6	The purpose of disclosure is marketing.	6.(2)
C7	The purpose of use is marketing.	6.(2)
C8	The consumer has given his explicit consent.	6.(2)
C9	The rules are laid down in section 6 of the Danish Marketing Act.	6.(2)
C10	Data are general data on customers.	6.(3)
C11	Data form the basis for classification into customer categories.	6.(3)

Table 2
A sample list of rights extracted from the data privacy regulations.

ID	Text	Constraints	Source
R1	Common processor may process personal data	$C1 \vee (C2 \wedge C3) \vee C4$	6.(1)
R2	A company may disclose data to a third company	$C5 \wedge C6 \wedge (C8 \vee (C10 \wedge C11))$	6.(2), 6.(3)
R3	A company may use data on behalf of a third company	$C5 \wedge C7 \wedge (C8 \vee (C10 \wedge C11))$	6.(2), 6.(3)

Table 3
A sample list of obligations extracted from the data privacy regulations.

ID	Text	Constraints	Source
O1	A company may not disclose data to a third company	$C5 \wedge C6$	6.(2)
O2	A company may not use data on behalf of a third company	$C5 \wedge C7$	6.(2)
O3	A company shall obtain the consent according to the rules	C9	6.(2)

part of the class *Natural person*, though they are both direct subclasses of the class *Body*.

The next step is to extract rights, obligations, and constraints with the help of the four patterns discussed previously. The biggest issue we encountered was that many of the paragraphs did not state any subject (cf. above). Another issue was the cross-references between subsections, which made us reuse complex logical expressions in many places. In the following we will provide a small excerpt from the document and apply the framework step by step. Some parts are removed from the excerpt and replaced with dots in order to decrease the level of complexity in this example.

> “6. (1) Personal data may be processed only if:
> the data subject has given his explicit consent; or
> processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or [...]”
>
> “(2) A company may not disclose data concerning a consumer to a third company for the purpose of marketing or use such data on behalf of a third company for this purpose, unless the consumer has given his explicit consent. The consent shall be obtained in accordance with the rules laid down in section 6 of the Danish Marketing Act.”
>
> “(3) However, the disclosure and use of data as mentioned in subsection (2) may take place without consent in the case of general data on customers which form the basis for classification into customer categories [...]”

We will first show the results after applying the framework and later on explain how these results were obtained. Note, the IDs of the rights, obligations, and constraints differ from the ones provided in Appendix A. Table 1 lists parts of the constraints, Table 2 – the rights, and Table 3 – the obligations.

We start applying the four patterns discussed earlier in order to extract rights, obligations, and constraints. We have first applied the basic activity pattern to form the right R1. As the subject is not stated we conclude that this right is associated with a new stakeholder – either a controller or a processor, which have the right to process data. We call this stakeholder a *common processor*. Next, we have a list of allowed circumstances (i.e., when data may be disclosed) for the right R1 in Section 6. (1). We apply the basic activity pattern everywhere to make sure we have only one subject, verb, and object. Based on that list of allowed circumstances in Section 6. (1) we identify the constraints C1, C2, C3, and C4. The purpose pattern is used to form the constraint C4 based on the “in order to” phrase in the text. Moreover, we apply the pattern to distinguish nouns by verb phrases to form the constraint C3 from the text “to which the data subject is party”. In Section 6. (2) we have a proper sentence with a subject – *a company*. We have two verbs here – *disclose* and *use*, and hence we form two obligations O1 and O2. These obligations are actually refrainments, as defined earlier, because they expressly state that the subject may not do something. Here we also apply the rule pattern, because we encounter the word “unless”. Therefore we add the two rights R2 and R3 as opposite to the obligations O1 and O2 respectively. The initial constraints for these rights are $C5 \wedge C6 \wedge C8$, however Section 6. (3) contains another exception of the obligations O1 and O2 and hence we extended the constraints for these rights.

When we have exceptions, e.g., “unless”, “if not”, “except”, we have to deal with them in a special manner. There are two possibilities – either use De Morgan’s law to update the constraint logic or involve prioritizations (Breaux et al., 2006). Prioritization is done by adding two more columns to the rights and obligations tables – *before* and *after*, which contain a list of rights/obligations (IDs) to look at before or after respectively. The relation between a before/after rights and obligations is of type logical OR. If we apply this method to the case discussed above, we would get $R2 \vee O1$, i.e. if the constraints for R2 are not satisfied, then the right R2 cannot be applied and we check the obligation O1. However, if the exception does not require a very complex change in the constraints, it is easier to apply De Morgan's law.

After applying the framework twice, we extracted 96 rights, 86 obligations, and 312 constraints. These can be seen in Appendix A.

4.2. Step (ii). Describe architectural requirements

A new cloud-based version of the Net4Care platform comes with added privacy concerns, therefore new privacy related functionality must be added. The Net4Care cloud platform will act as data processor with respect to the private data uploaded via the Net4Care services. Net4Care acts as an intermediate layer between the cloud storage and the client using the telemedical ecosystem through the API provided. While Net4Care itself does not assume the role of data controller, the entity that installs and uses Net4Care in the context of cloud computing has to assume a data controller role. Net4Care should provide functionality for the data controller such as logging, information retrieval and access, deletion, etc., in order to aid the developer using Net4Care to fulfill legal obligations.

The registration of a new application requires the developer to sign up a contract, i.e., accepting terms of service, in accordance with requirement QS-D4 (see below). These terms of service stipulate that the developer is responsible to take care of data that the developer or the users of the application fetch from Net4Care. Although Net4Care can track who accesses what, possible misuse of this data cannot be prevented. In this context developers should be responsible for their actions and should also take the necessary precautions when dealing with personal data. In order to delegate these responsibilities, Net4Care acts as a data processor as described in Section 2.1, and thus leaving the developers and end-users to act as data controllers.

The Net4Care platform has to provide role-based access as we discuss when formulating the new requirements based on the regulations. There should be at least four distinct roles of users to Net4Care: Developer, Administrator, Patient, and Healthcare professional.

Based on the legal text and by extracting the stakeholders, rights, obligations and constraints, we can formulate a set of functional and non-functional requirements that (a cloud-based) Net4Care needs to fulfill in order to be compliant with the privacy law. We proceed from the obligations and rights that state what the processor **should do** or how the system **should be** and decide if this can be formulated as a functionality or quality of the system, respectively. We take into account the constraints for the right or obligation and add these as system state, system environment, or stimuli. This is a non-formal process with which to extract requirements, but we will use this as a starting point to form the requirements; and later use the goal oriented framework (see Section 2.3) to argue that the requirements formulated are in compliance with the legal regulations.

Some of the new requirements will not have a direct correspondent in the rights and obligations extracted by the modeling framework, as not all legal texts were formally modeled; such as the Executive Order on Security (Datatilsynet, 2011a) and the Healthcare Law (Indenrigs- og Sundhedsministeriet, 2010). Nevertheless, we included requirements based on those laws, as we consider that they cover essential functionality or qualities for a healthcare software platform.

Moreover, as we are involving cloud computing, it is important to create a separation between the cloud provider and Net4Care. This means that in case of, e.g., increase in price, Net4Care can be installed on another cloud provider and this should not break its functionality. Affected data, should be migrated separately.

QS-D4. Developer Contractual Agreement	
Overview	Legal binding between Net4Care and SME Developer. Net4Care (the processor) must provide processor-controller contractual agreements that the SME Developer (controller) using the platform must accept in order to use the system.
Rights and Obligations references	O58, O57, O59
System State	The Net4Care system has not been set up for the Developer.
System Environment	The developer has not yet started using the system.
Environment changes	The SME developer wants to start using the Net4Care system (use the API or wants to develop a new component) and does so by registering on a Net4Care registration platform.
Required system behavior	In order to have access to the development platform, Net4Care must first issue a contractual agreement with the SME developer that he/she must accept.

QS-U8. Safe Harbor requirement	
Overview	Data gathered by Net4Care shall be stored and transferred only in the EU or countries that respect the Safe Harbor agreement.
Rights and Obligations references	R40, R41, O24
System State	The Net4Care system is running normally.
System Environment	Measurements are being stored on the Net4Care system.
Environment changes	The cloud provider decides that copies of the data need to be made, or that the data should be moved to another data center .
Required system behavior	The data will end up being stored in another EU country or a country that respects the Safe Harbor Agreement.

QS-U9. Disclosure to third-parties	
Overview	Data gathered by Net4Care shall not be disclosed to other third parties; the data shall only be stored in the Net4Care system.
Rights and Obligations references	R14, O15, O16
System State	The Net4Care system is running normally.
System Environment	Measurements have been stored on the Net4Care system.
Environment changes	Any action that requires storing data in Net4Care.
Required system behavior	The system guarantees that data shall remain stored only on the Net4Care servers.

FS-U3. Patient accesses her data	
Overview	Patient access records. Patient shall only be able to access her own records.
Rights and Obligations references	O30, O31, O32, O33, Healthcare Law (Indenrigs- og Sundhedsministeriet, 2010)
System State	The Net4Care system is running normally.
System Environment	Patient is registered with the Net4Care's Authentication system.
Environment changes	Patient wants to access measurements on the Net4Care's system that do not belong to him or for which he has not been granted access.
Required system behavior	Net4Care disallows this action and logs the unauthorized access.

FS-U4. Disclosing data	
Overview	Patient can explicitly allow or disallow other Net4Care users to access her data.
System State	The Net4Care system is running normally.
Rights and Obligations references	Healthcare Law (Indenrigs- og Sundhedsministeriet, 2010). Chapter 9
System Environment	Patient is registered to the Net4Care's Authentication system.
Environment changes	Patient gives consent to another Net4Care user (patient or healthcare professional) to access data.

(*continued*)

FS-U4. Disclosing data	
Required system behavior	The Net4Care system makes a note of this and will allow access for the consented user to the data of the patient in 8 hours (configurable time period).
FS-U5. Personal data rectification	
Overview	A patient can modify or delete her observations if a justified objection has been filed against the data controller. The system provides this rectification functionality.
Rights and Obligations references	O47
System State	The Net4Care system is running normally.
System Environment	Patient is registered to the Net4Care's Authentication system and has uploaded measurements.
Environment changes	Patient objects to the data processing. Patient wants to modify or delete measurements.
Required system behavior	The system must provide a way to alter and delete measurements.
FS-U6. Data logging	
Overview	An authority(patient, healthcare professional or legal authority) requires access to a patient's measurement history through logs on the system for a legal matter.
Rights and Obligations references	Datatilsynet Executive order on security (Datatilsynet, 2011a) Section 19(1)
System State	The Net4Care system is running normally.
System Environment	Patient is registered to the Net4Care Authentication system and has uploaded measurements.
Environment changes	An authority wants access to the logs of a patient's records for a legal matter.
Required system behavior	The Net4Care system keeps a log of all measurements uploaded or deleted.
FS-U7. Healthcare professional measurements access	
Overview	A healthcare professional can only access patient measurements for the patients under his treatment.
Rights and Obligations references	Health Act (Indenrigs- og Sundhedsministeriet, 2010). Chapter 9
System State	Net4Care system working normally.
System Environment	A registered healthcare professional has a set of patients registered with the Net4Care authentication system.
Environment changes	Healthcare professional wants to access measurements on the Net4Care system that do not belong to his patients or for which he has not been granted access.
Required system behavior	Net4Care disallows this action and logs the unauthorized access.
FS-U8. Restricted Access Attempts	
Overview	When multiple failed authentication attempts from the same source have been initiated, or when trying to access a measurement without proper authentication from the same source the system should log this and temporarily prevent that source from initiating any more requests.
Rights and Obligations references	Datatilsynet Executive order on security (Datatilsynet, 2011a) Section 18
System State	The Net4Care system is running normally.
System Environment	Patient is registered to the Net4Care's Authentication system and has uploaded measurements.
Environment changes	A unauthenticated source wants to access measurements on the Net4Care platform.
Required system behavior	The Net4Care platform blocks access attempts from that source after 5 unsuccessful attempts for 8 hours.

4.3. Step (iii). Make the GSN argument

We will construct two separate modules containing the argumentation for compliance. These two modules are linked in the general goal – our hypothesis. Fig. 4 shows the general GSN model we have created. The topmost goal of our argument is that Net4Care complies with the privacy regulations. This is with purpose very broad as it states what we want to achieve with our system. Moreover, we define the context for our topmost goal – e.g., the software requirement, along with attaching some starting-point assumptions – e.g., that we have defined all necessary requirements. This context is automatically derived by other subgoals and strategies we are going to define further in the model tree. In order to establish our main claim, we split it into two subgoals – each presenting one of the necessary arguments as discussed earlier (cf. Section 3). The global context for our argumentation contains: the set of all Net4Care requirements, the Act on Processing Personal Data, the Executive Order on Security, and the Health Care Act. Some important assumptions have to be made in advance as well. These include, e.g., that Net4Care acts as data processor as defined the Act on Processing Personal Data (Datatilsynet, 2013). This will be used throughout the entire argumentation process. We also have to assume that our regulations model is correct and we have connected the identified rights and obligations to the requirements properly.

The first module, M1, contains correctness argumentation, i.e., arguments that requirements are permitted by the regulations. Regulations are represented by the rights and obligations we extracted from the regulatory document (see 2.2). We justify this argumentation by representing each requirement as a separate goal. The context consists primarily of pointers to the rights and/or obligations in the regulations' model. As we have not applied the modeling framework to the Executive Order on Security and the Health Care Act, we refer directly to a specific section within these two acts. Solutions, attached to goals that represent requirements, give evidence on how exactly we argue that the requirement is permitted by the regulations (stated as a context). Fig. 5 visualizes the module M1 with its topmost goal M1:G1 along with the strategy described above (S1) and one of the requirements (QS-U1) mapped as a goal G2. The full model is presented in Appendix B.

The second module, M2, contains completeness argumentation, i.e., arguments that the privacy regulations are concerned by Net4Care's requirements. We will justify this by going through each obligation from our mapping (see Section 2.2). We have to take only those obligations, whose constraints match our case, i.e. data is private data, data concerns health life, or the actor is the processor or common processor as explained in Section 2.1. The solutions, in terms of GSN, to our goals are these requirements that make sure the system does not abuse the obligations in the goals. Fig. 6 shows the module M2 with its topmost goal M2:G1 along the strategy described above (S1) and with four obligations mapped to a requirement, making sure the system takes these obligations into consideration. The full model is presented in Appendix B.

Note that all objects in the two modules are internal to the module. For example, strategy S1 in module M1 is different from strategy S1 in module M2. The module prefix in the identifier is omitted for simplification.

Moreover it is interesting to pay attention to how solutions are defined in both modules. When arguing correctness (see M1) the solutions are the real means of how we will ensure the compliance by applying certain mechanisms (e.g., secure transfer over the network, and data and access logging). On the other hand, when arguing completeness (see M2), the solutions refer to the actual software requirement that takes into consideration the related rights and obligations.

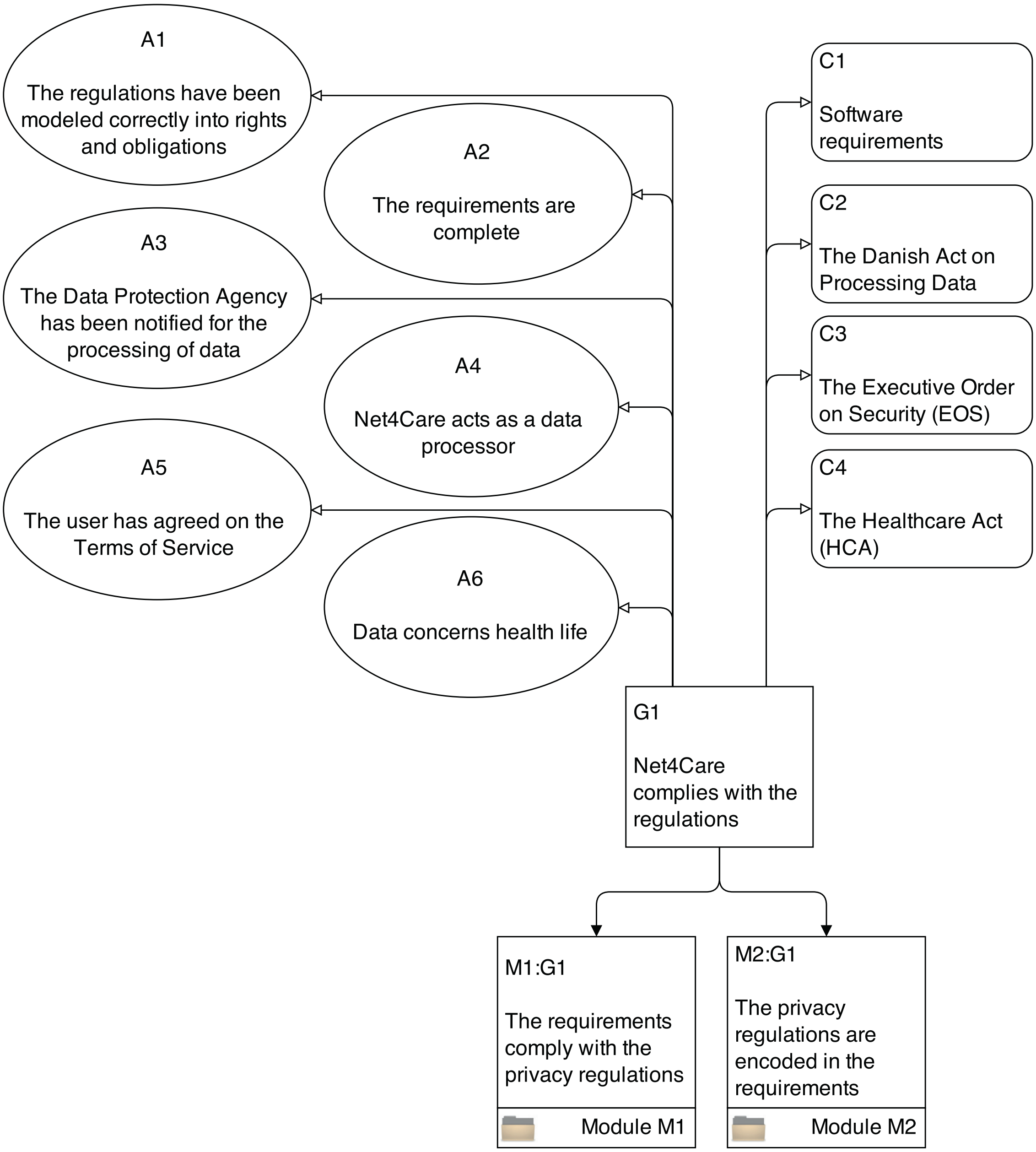
A1
The regulations have been modeled correctly into rights and obligations
A2
The requirements are complete
A3
The Data Protection Agency has been notified for the processing of data
A4
Net4Care acts as a data processor
A5
The user has agreed on the Terms of Service
A6
Data concerns health life
C1
Software requirements
C2
The Danish Act on Processing Data
C3
The Executive Order on Security (EOS)
C4
The Healthcare Act (HCA)
G1
Net4Care complies with the regulations
M1:G1
The requirements comply with the privacy regulations
Module M1
M2:G1
The privacy regulations are encoded in the requirements
Module M2

Fig. 4. GSN general model. It shows the topmost goal along with the two important subgoals.

4.4. Step (iv). Conclude

The current version of Net4Care is not compliant with the privacy regulations if it was to be deployed in the cloud. The current issues with regard to this are:

- Secure data deletion – when data is no longer needed;
- Logging – log access to the data;
- Data disclosure – who is accessing what (need to impose strict roles).

By implementing the new requirements discussed above we argue that Net4Care could be securely deployed in the cloud, in particular in the Microsoft Azure cloud since it complies with the EU Safe Harbor agreement, without contradicting with any regulation while in the same time fulfilling the most important rights and obligations in order to support the law fully. To support our claim we develop a GSN model, one can use to potentially argue that Net4Care complies with the privacy regulations.

Although this model is not verified by legal experts, it relates an understanding of how the system requirements are developed to cover the regulations analyzed. We do not claim we have completely covered the legislative documents, but rather state that we have established a formal way of justifying whether a software architecture complies with regulations. The developed GSN model can further be used as a part of Net4Care's terms of service in order to reason about its compliance with the regulations.

It is also possible to argue that an application built on top of Net4Care complies with the privacy regulations. Such an application can reuse the developed GSN model as a separate module in order to provide such an argument. However, applications built on top of Net4Care should also provide their own arguments on why they are regulation-compliant, e.g., one application can read data and then disclose it to third parties without a consent from the data subject, which does not fulfill a privacy obligation. Further-

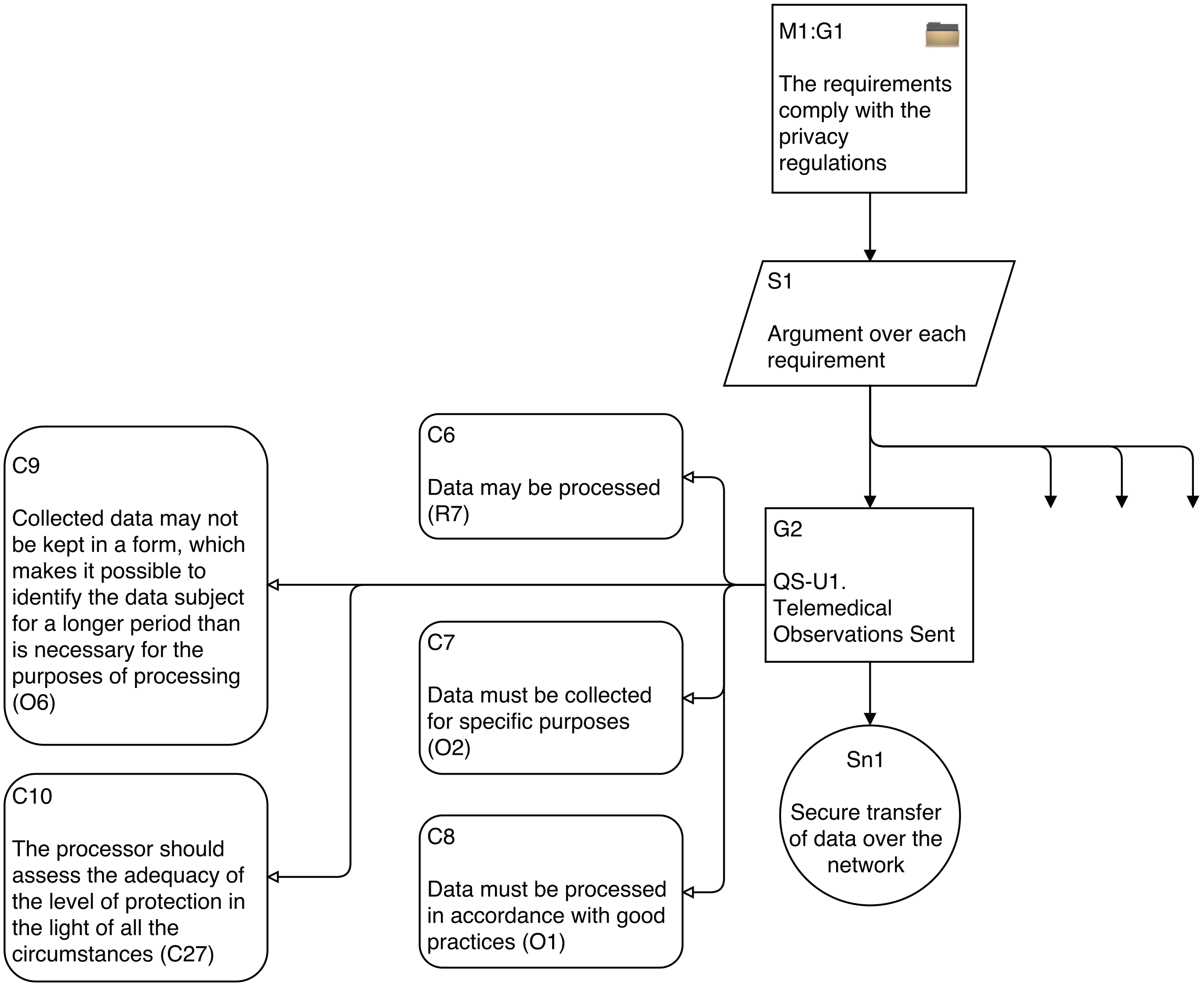
M1:G1
The requirements comply with the privacy regulations
S1
Argument over each requirement
G2
QS-U1. Telemedical Observations Sent
Sn1
Secure transfer of data over the network
C6
Data may be processed (R7)
C7
Data must be collected for specific purposes (O2)
C8
Data must be processed in accordance with good practices (O1)
C9
Collected data may not be kept in a form, which makes it possible to identify the data subject for a longer period than is necessary for the purposes of processing (O6)
C10
The processor should assess the adequacy of the level of protection in the light of all the circumstances (C27)

Fig. 5. GSN argument for correctness. The topmost goal is shown along with the requirement QS-U1.

more, these applications should decide their role according to the legislation, e.g., a data processor or a data controller.

Last but not least, internal Net4Care developers, who continue to maintain and develop the ecosystem, must be disciplined enough so that their changes do not contradict with privacy regulations. This can be assured by, e.g., regular code reviews, so that issues can be detected at an early stage.

5. Related work

Breaux and Antón introduced the Semantic Parameterization process that takes a fundamental part in our work, as described in Section 2.2. As an extension to this work, Breaux and Gordon introduced the Legal Requirements Specification Language (LRSL) – a special language to encode regulative texts (Breaux and Gordon, 2013). This language allows analysts to restate legal texts into rights and obligations, to create links between regulations (both between paragraphs within one document and between different documents), and to support traceability back to the original content. Furthermore, LRSL-encoded regulations can be processed by an automated parsing tool that can check for syntax (e.g., unassociated logical expressions) and semantic errors (e.g., incorrect references). The parser-constructed model can then be used to browse the legal texts and run different queries on them. Last but not least the model can be exported to other formats, such as the HyperText Markup Language (HTML) and Graph Markup Language (GraphML).

Although we have manually processed all the regulatory documents, an automated tool could also have be applied. Kiyavitskaya et al. (2007) adapt the Cernoś framework to the healthcare domain and run a tool to automatically extract rights, obligations, and their constraints from HIPAA. Due to lack of a golden reference to compare the results to, we have omitted this possibility as it would have required us to manually verify the output. Moreover, the tool has some lexical limitations, which make the final outcome deviate from an optimal one.

Another related process is presented by Islam et al. in their framework to support alignment of secure software engineering with legal regulations (Islam et al., 2011). Their approach consists of four steps:

1. *Create a model of the regulations* to support the understanding of the concerned regulatory texts. The output is similar to what Semantic Parameterization does in the sense that a set of lan-

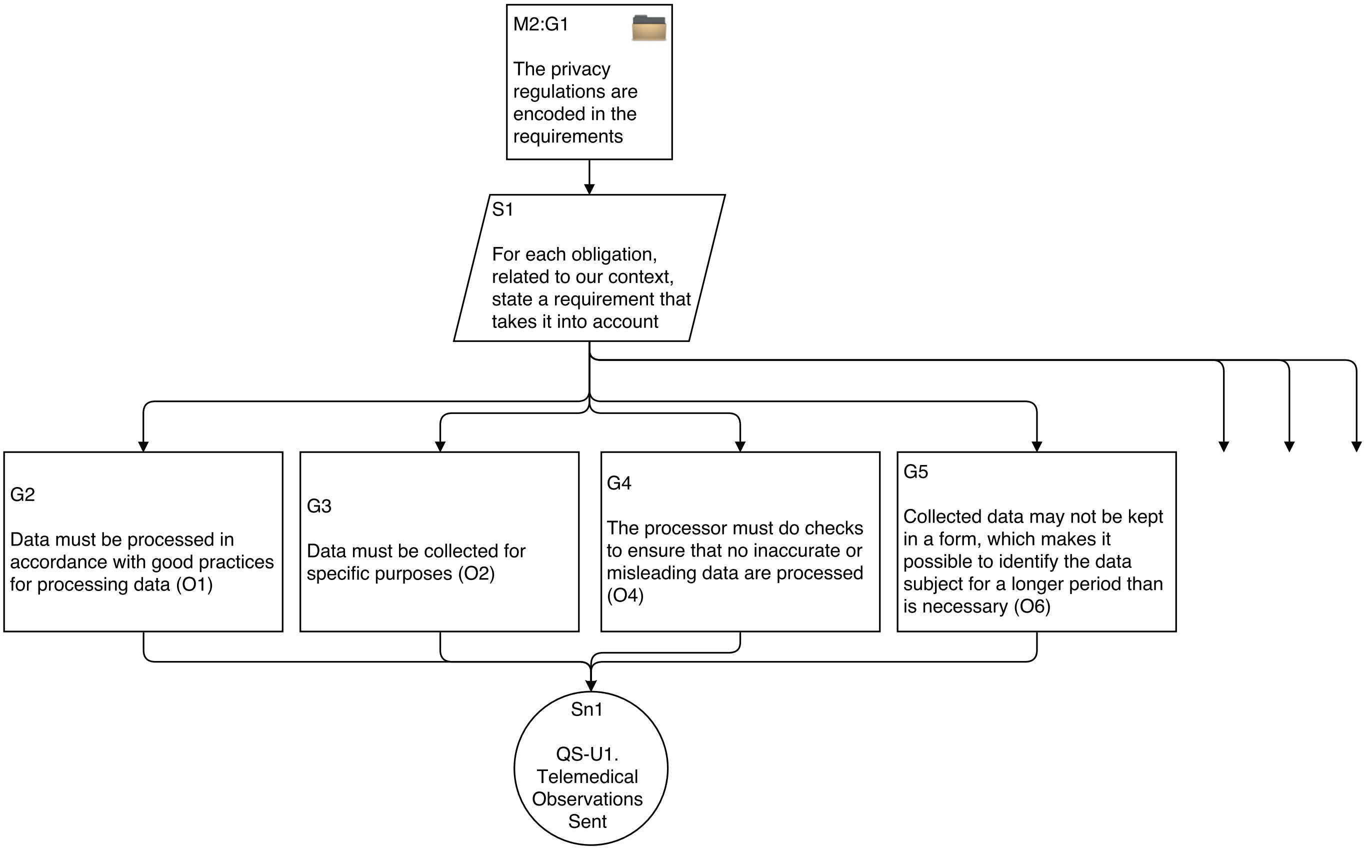
M2:G1
The privacy regulations are encoded in the requirements
S1
For each obligation, related to our context, state a requirement that takes it into account
G2
Data must be processed in accordance with good practices for processing data (O1)
G3
Data must be collected for specific purposes (O2)
G4
The processor must do checks to ensure that no inaccurate or misleading data are processed (O4)
G5
Collected data may not be kept in a form, which makes it possible to identify the data subject for a longer period than is necessary (O6)
Sn1
QS-U1. Telemedical Observations Sent

Fig. 6. GSN argument for completeness. The topmost goal is shown along with four obligations and their corresponding requirements.

guage patterns is applied which results in an extraction of possible legal rights (e.g. claim, privilege, power, immunity) and their correlatives (e.g. duty, no-right, liability, disability).

2. *Elicit security requirements* based on the output from the previous step and a security analysis of the system under development.
3. *Analyze security requirements* in order to identify potential threats that might lead to non-compliance in the system under development.
4. *Create a system design* that illustrates how the system under development fulfills the identified security requirements and legal constraints.

The resulting model from this framework is based on the Unified Modeling Language (UML). The focus here is put on the security aspects of a system under development with respect to regulations – how to prevent external attackers breaking into the system and hence putting it into a non-compliant state. In contrast to Islam et al., we focus on the argument that the software architecture of a system complies with (security) regulations.

Essential part of our work lies in the construction of a compliance argument that can be used to assure that a system complies with a set of regulations. Graydon et al. (2012) propose "using explicit, rigorous, and structured conformance arguments to transfer confidence in software integrity." According to their work the compliance assessment should be "both predictable and repeatable", which currently is very hard achieved. Even if a company hires a 3rd-party to do the assessment, the process is not 100% repeatable as there is no algorithm to be used. Graydon et al. argue about the creation of a "conformance argument" as a new approach of transferring confidence. These arguments should be necessarily informal and logical. As developers know the system they are building in their bones, they should also be aware of external legislation factors that may constrain the development process in a way. It is further developers that have to argue about the system compliance with the regulations, so the argument is actually developers' interpretation of these regulations. By applying a graphical framework like the Goal Structuring Notation (Kelly and Weaver, 2004) we can create a logical tree of claims that end with a definite evidence that supports the claims in its branch. This tree can later be reused and updated with more details when necessary.

The Goal Structuring Notation (GSN; (Kelly and Weaver, 2004)) has primarily been used to describe the structure of safety cases. We use this argumentation approach to argue for general regulation compliance since in addition to a primary argument, the notation focuses on the context in which the argument applies. This maps well to the contexts identified in Semantic Parameterization. Sujan et al. (2007) explicitly applied GSN to a healthcare context but did not consider security, nor systematically considered modeling of regulations. Vivas et al. (2011) introduced a model-driven approach for security assurance that used "assurance cases" that is based on GSN. The approach does, however, not take regulations systematically into account. Similarly, He and Johnson (2012) directly used GSN to make security arguments, but also did not consider models of regulations.

A similar goal-based approach, called Goal-driven Security Risk Management, is also employed by Islam et al. (2010). The approach "explicitly models the relations between the goals based on the software development components and project success indicators with the risk factors that obstruct these goals." Islam (2009) Ghanavati et al. point to User Requirements Notation – a standard, which "combines goals and scenarios in order to help capture, model, and analyze user requirements in the early stages of development." Ghanavati et al. (2007) To this standard there are two supplementary notations – Goal-oriented Requirement Language and Use Case Maps, that together create relationships between goals and business processes.

6. Conclusions

This article presents an approach for arguing that a system implemented according to a software architecture design fulfills regulatory requirements. The approach applies Semantic Parameterization to regulatory texts and integrates the rights and obligations derived from it with a Goal Structuring Notation (GSN) argument for compliance in which software architecture decisions appear as supporting evidence.

Important part of this work is to make the entire compliance argument visible and understandable (and hence easily discussable). By applying GSN we aim to create an argument foundation – a model that can be used, e.g., when signing a contract for a project or when assessing the compliance level of a given system. We argue that the model is rigorous and logical and can be examined by 3rd-parties. This model, thought, have a lot of preconditions that must be in place in order the logic inside to be correct. This could be for example that developers adhere to the regulatory constraints and maintain compliant code. Moreover, the model must incorporate both the software requirement and the legislative texts (in the form of rights and obligations) in order to argue compliance. Therefore, we have chosen to split the model into two sub-models – one arguing completeness and one arguing correctness. This way we ensure that both of the artifacts, the requirement or the legislative texts, are viewed as a starting point. By visualizing the argument logic in a simple and understandable way (such as by the means of GSN) one could easily see the essence of the compliance. One could further elaborate on this logic or accept it as satisfactory.

When developers are working on the system implementation, it is necessary to maintain a certain working culture in order to support the compliance of the system. A developer can easily implement a given software requirement in a way that is not allowed by regulations. To prevent this piece of code going into production, a certain degree of reviewing is necessary. One could for example apply code review for every change in the code and disallow improper code to be committed into the version control system. This activity requires though the reviewer to be aligned with the legislative norms. When working with legal compliance, the entire organization should be set in a way to support it – from developers, through testers, to project managers and support.

An important concern is whether the reviewer performs a fair review. If working in the same organization, he could be tempted (or forced) to approve code that is against the legislation. Another option could be that an external party performs the code review instead, but this still does not give 100% guarantee the review is fair. A recent case of the manipulation of the test results by Volkswagen (U.S. Environmental Protection Agency, 2015) is an example that contracts and results that go public are not a guarantee for the actual work performed. In this sense the GSN model we present is a tool to ease the compliance enforcement, but not a guarantee the developed system is indeed compliant.

We reported on the application of this approach to the cloud migration of Net4Care and specifically considered the Danish (and European) privacy regulations in relation to this. The initial situation was such that Net4Care was a stand-alone application that worked extensively with private data – healthcare data primarily. Our goal was to argue whether we could migrate the application to a cloud environment so that it was used as Software-as-a-Service and hence removing the burden of installing and maintaining it. Aside from the technical challenges, our concern was how to address the legal part. By applying the steps described in this paper, developers gained substantial knowledge in the legal domain and could make the relation between the initial software requirements and the additional legal ones (in form of rights and obligations) visible. This enables them to make important architectural decisions already in the beginning of a project to support the compliance at a later stage. The model itself could be used as a proof when an organization becomes interested in using Net4Care. An important remark to our approach is that a legal person should be involved in the process in order to verify the produced model. But we argue that having such a foundation would make the verification process more explicit for both sides – the legal and the technical. Furthermore, as discussed above, it is important to create a culture in the organization to develop a system that complies with regulations and to maintain it later. We concluded that Net4Care needs change in order to support cloud migration, but that migration to the Microsoft Azure cloud is indeed possible.

Acknowledgments

The work has been partially supported by the SCAUT project financed by Innovation Fund Denmark, grant 72-2014-1.

Appendix A. Rights and obligations extracted from privacy regulations

In the following we present the full results from the extraction of rights and regulations we have applied to the data privacy regulations in Denmark. The following is a list with all stakeholders we have identified from the legal text:

- Controller
- Processor
- Common processor
- The Minister of Justice
- The supervisory authority
- A body
- Administrative authorities
- Private bodies (private individuals)
- Private persons
- Official authorities
- Public authority
- Private company
- The Data Protection Agency
- Controller's representative
- A data subject
- A competent Minister
- The Minister of Interior
- The Council
- Members/Staff of Datatilsynet
- A non-profit-seeking body (foundation, association or any other)
- A company

A1. Constraints

Here we list all the constraints that we have identified. Each constraint has a unique identifier (ID). Some of the constraints begin with underscore, which means they are expressed with other constraints. The reason we keep some of these constraints is that the actual expression is complex and it makes sense for us to keep a simpler version in the list.

ID	Text	Source
C1	The purposes of data collection are specified, explicit and legitimate	5. (2)
C2	Further processing must not be incompatible with the purposes	5. (2)
C3	Historical, statistical or scientific purposes shall not be considered incompatible with the purposes	5. (2)
C4	Data must be adequate and relevant	5. (3)
C5	Data must not be excessive in relation to the purposes of collection	5. (3)
C6	Data must not be excessive in relation to the purposes of the subsequent processing	5. (3)
C7	The way of processing data ensures the required updating of the data	5. (4)
C8	Checks are made to ensure that no inaccurate or misleading data are processed	5. (4)
C9	Data turn out to be inaccurate or misleading	5. (4)
C10	The form makes it possible to identify the data subject for a longer period than is necessary for the purposes of processing	5. (5)
C11	The data subject has given his explicit consent for the processing of personal data	6. (1), 7. (2), 7. (4), 8. (4)
C12	Processing of personal data is necessary for the performance of a contract	6. (1)
C13	The data subject is party to a contract	6. (1)
C14	Processing of personal data is necessary in order to take steps at the request of the data subject prior to entering into a contract	6. (1)
C15	Processing of personal data is necessary for compliance with a legal obligation	6. (1)
C16	The controller is subject to a legal obligation	6. (1)
C17	Processing of personal data is necessary in order to protect the vital interests of the data subject	6. (1)
C18	Processing of personal data is necessary for the performance of a task	6. (1)
C19	The task is carried out in the public interest	6. (1)
C20	The task is carried out in the exercise of official authority	6. (1)
C21	The official authority is vested in the controller	6. (1)
C22	The task is carried out in a third party	6. (1)
C23	The data are disclosed to the third party	6. (1), 37. (2)
C24	Processing of personal data is necessary for the purposes of the legitimate interests	6. (1)
C25	The legitimate interests are pursued by the controller	6. (1)
C26	The legitimate interests are pursued by the third party	6. (1)
C27	The legitimate interests are not overridden by the interests of the data subject	6. (1)
C28	Data concern a customer	6. (2)
C29	Data is disclosed for the purpose of marketing	6. (2), 36. (1)
C30	Data is used for the purpose of marketing	6. (2), 36. (1)
C31	The consumer has given his explicit consent for the disclosing of data	6. (2),
C32	The consumer has given his explicit consent for the using of data	6. (2)
C33	The rules are laid down in section 6 of the Danish Marketing Act	6. (2), 36. (3)
C34	Data are general data on customers	6. (3)
C35	Data form the basis for classification into customer categories	6. (3)
_T1	the conditions laid down in subsection (1) 7 are satisfied	6. (3)
_T2	Data is of the type mentioned in sections 7 and 8	
C36	Data reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership	7. (1)
C37	Data concern health or sex life	7. (1)
C38	Processing of personal data is necessary to protect the vital interests of the data subject	7. (2)
C39	Processing of personal data is necessary to protect the vital interests of other person than the data subject	7. (2)
C40	The data subject is physically or legally incapable of giving his consent	7. (2)
C41	The other person is physically or legally incapable of giving his consent	7. (2)
C42	The data subject has made the data public	7. (2)
C43	The processing of personal data is necessary for the establishment, exercise or defense of legal claims	7. (2)
C44	Data concern trade union membership	7. (3)
C45	The processing of personal data is necessary for the controller's compliance with labor law obligations or specific rights	7. (3)
C46	The aim is a political, philosophical, religious or trade-union	7. (4)
_T3	data is mentioned in subsection (1)	7. (4)
C47	Data relate to the members of the body	7. (4)
C48	Data relate to persons	7. (4)
C49	Persons have regular contact with the body in connection with the purposes of the body	7. (4)
_T4	the processing is covered by subsection (2) 2 to 4 or subsection (3).	7. (4)
C50	Processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services	7. (5)
C51	Data are processed by a health professional subject	7. (5)
C52	The health professional subject is under law to the obligation of professional secrecy	7. (5)
C53	The processing of personal data is required for the performance by a public authority of its tasks in the area of criminal law	7. (6)
C54	The processing of data takes place for reasons of substantial public interests	7. (7)
C55	The automatic registers contain data on political opinions	7. (8)
C56	Data are not open to the public	7. (8)
C57	Data is about criminal offences, serious social problems or other purely private matters	8. (1)
_T5	The private matters differ from those mentioned in section 7 (1)	8. (1)
C58	The processing of data is necessary for the performance of the tasks of the administration	8. (1)
C59	Data is processed on behalf of a public administration	8. (2)
C60	Disclosure takes place for the purpose of pursuing private or public interests	8. (2)
C61	The interests clearly override the interests of secrecy, including the interests of the related person	8. (2)
C62	Disclosure is necessary for the performance of the activities of an authority	8. (2)

(*continued on next page*)

(*continued*)

ID	Text	Source
C63	Disclosure is required for a decision to be made by an authority	8. (2)
C64	Disclosure is necessary for the performance of tasks for an official authority by a person or a company	8. (2)
C65	Administrative authorities perform tasks in the social field	8. (3)
_T6	Data is mentioned in section 7. (1)	8. (3)
_T7	the conditions laid down in subsection (2) 1 or 2 are satisfied	8. (3)
C66	The disclosure is a necessary step in the procedure of the case	8. (3)
C67	The disclosure is necessary for the performance by an authority of its supervisory or control function	8. (3)
C68	Processing is necessary for the purpose of pursuing a legitimate interest	8. (4)
C69	The interest clearly overrides the interests of the data subject	8. (4)
C70	Disclosure is for the purpose of pursuing public or private interests, including the interests of the person concerned, which clearly override the interests of secrecy	8. (5)
C71	The interests clearly override the interests of secrecy	8. (5)
_T8	(C11 – ((C38 & C40) – (C39 & C41)) – C42 – C43) – (C44 & C45) – (C46 & ((C36 – C37) & (C47 – (C48 & C49)))) – (((C36 – C37) & (C47 – (C48 & C49))) & (C11 – (((C38 & C40) – (C39 & C41)) – C42 – C43 – (C44 & C45)))) – ((C36 – C37) & C50 & C51 & C52) – ((C36 – C37) & C53)	8. (6)
_T9	Data as mentioned in section 8	9. (1)
C72	The processing of data is carried out for the sole purpose of operating legal information systems of significant public importance	9. (1)
C73	The processing of data is necessary for operating legal information systems of significant public importance	9. (1)
C74	The processing of data is carried out solely for the purpose of operating legal information systems	9. (2), 9. (3), 45. (1), 50. (1)
_T10	data mentioned in section 6	9. (3)
C75	The processing of data takes place for the sole purpose of carrying out statistical or scientific studies of significant public importance	10. (1)
C76	The processing of data is necessary in order to carry out statistical or scientific studies of significant public importance	10. (1)
C77	The processing of data takes place for the sole purpose of carrying out statistical or scientific studies	10. (2)
C78	The disclosure if authorized by the supervisory authority	10. (3)
C79	The conditions concern the disclosure of data	10. (3)
C80	Data concern identification numbers	11. (1)
C81	Data are with a view to unambiguous identification or as file numbers	11. (1)
C82	The processing of data follows from law or regulations	11. (2)
C83	The data subject has given his explicit consent for the processing of data	11. (2), 12. (1)
C84	The processing of data is carried out solely for scientific or statistical purposes	11. (2), 45. (1)
C85	The processing of data is a matter of disclosing an identification number	11. (2)
C86	The disclosure of data is a natural element of the ordinary operation of companies, etc. of the type mentioned	11. (2)
C87	The disclosure of data is of decisive importance for an unambiguous identification of the data subject	11. (2)
C88	The disclosure of data is demanded by an official authority	11. (2)
C89	Controller sells lists of groups of persons for marketing purposes	12. (1)
C90	Controller performs mailing or posting of messages to such groups on behalf of a third party	12. (1)
C91	Data concern name, address, position, occupation, e-mail address, telephone and fax number	12. (1)
C92	Data is contained in trade registers	12. (1)
C93	The trade registers according to law or regulations are intended for public information	12. (1)
C94	Calls are made from telephones of the public authority to other telephones	13. (1)
C95	Calls are made from telephones of the private company to other telephones	13. (1)
C96	The supervisory authority has provided a prior authorization for the carrying out of automatic registration of the telephone numbers	13. (1)
C97	Important private or public interests speak in favor of the telephone numbers	13. (1)
C98	The registration of numbers is provided by the law	13. (2)
C99	The registration is of numbers either for own use or for use in connection with technical control	13. (2)
C100	The numbers are called by suppliers of telecommunications networks and by teleservices	13. (2)
C101	Data is covered by the Act	14.
C102	The rules are laid down in the legislation on archives	14.
C103	The third country in question ensures an adequate level of protection	27. (1)
C104	The protection is afforded by a third country	27. (2)
C105	The circumstances surround a data transfer operation	27. (2)
C106	The circumstances include the nature of the data, the purpose and duration of the processing operation, the country of origin and country of final destination, the rules of law in force in the third country in question and the professional rules and security measures which are complied with in that country	27. (2)
C107	The data subject has given his explicit consent for the transfer to a third country	27. (3)
C108	The transfer of data to a third country is necessary for the performance of a contract between the data subject and the controller	27. (3)
C109	The transfer of data to a third country is necessary for the implementation of precontractual measures	27. (3)
C110	The precontractual measures are taken in response to the data subject's request	27. (3)
C111	The transfer of data to a third country is necessary for the conclusion or performance of a contract between the controller and a third party	27. (3)
C112	The contract is concluded in the interest of the data subject	27. (3)
C113	The transfer of data to a third country is necessary or legally required on important public interest grounds	27. (3)
C114	The transfer of data to a third country is necessary or legally required for the establishment, exercise or defence of legal claims	27. (3)
C115	The transfer of data to a third country is necessary in order to protect the vital interests of the data subject	27. (3)

(*continued on next page*)

(*continued*)

ID	Text	Source
C116	The transfer of data to a third country is made from a register	27. (3)
C117	The register according to law or regulations is open to consultation to the extent that the conditions are fulfilled in the particular case	27. (3)
C118	The consultation is done either by the public in general or by any person	27. (3)
C119	The conditions are laid down in law	27. (3)
C120	The conditions are for consultation	27. (3)
C121	The person can demonstrate legitimate interests	27. (3)
C122	The transfer of data to a third country is necessary for the prevention, investigation and prosecution of criminal offences	27. (3)
C123	The transfer of data to a third country is necessary for the execution of sentences	27. (3)
C124	The transfer of data to a third country is necessary for the protection of persons charged, witnesses or other persons in criminal proceedings	27. (3)
C125	The transfer of data to a third country is necessary to safeguard public security, the defence of the Realm, or national security	27. (3)
C126	The controller adduces adequate safeguards with respect to the protection of the rights of the data subject	27. (4)
C127	The carrying out of the transfer is on the basis of contracts in accordance with the standard contractual clauses	27. (5)
C128	The contractual clauses are approved by the European Commission	27. (5)
C129	The personal data have been collected from the data subject	28. (1)
C130	The information contains the identity of the controller	28. (1)
C131	The information contains the identity of the controller and of his representative	28. (1), 29. (1)
C132	The information contains the purposes of the processing data	28. (1), 29. (1)
C133	The information is necessary to enable the data subject to safeguard his interests	28. (1), 29. (1)
C134	The information have regard to the specific circumstances in which the personal data are collected	28. (1), 29. (1)
C135	The information contains the categories of recipients	28. (1), 29. (1)
C136	The information contains whether replies to the questions are obligatory or voluntary, as well as possible consequences of failure to reply	28. (1), 29. (1)
C137	The information contains the rules on the right of access to and the right to rectify the data relating to the data subject	28. (1), 29. (1)
C138	The personal data are collected in the specific circumstances	28. (1), 29. (1)
C139	The data subject already has the information	28. (2), 29. (2)
C140	The data have not been obtained from the data subject	29. (1)
C141	The information is provided at the time of undertaking the registration of the data	29. (1)
C142	The information is provided when the disclosure to a third party is envisaged	29. (1)
C143	The information is provided no later than the time when the data are disclosed	29. (1)
C144	The information contains the categories of data concerned	29. (1)
C145	The recording or disclosure of data is expressly laid down by law or regulations	29. (2)
C146	The provision of such information to the data subject proves impossible	29. (3)
C147	The provision of such information to the data subject would involve a disproportionate effort	29. (3)
C148	The data subject's interest in obtaining the information is found to be overridden by essential considerations of private interests	30. (1)
C149	The considerations of private interests include the consideration for the data subject himself	30. (1)
C150	The data subject's interest in obtaining this information is found to be overridden by essential considerations of public interests	30. (2)
C151	Public interests are national security	30. (2)
C152	Public interests are defence	30. (2)
C153	Public interests are public security	30. (2)
C154	Public interests are the prevention, investigation, detection and prosecution of criminal offences	30. (2)
C155	Public interests are the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions	30. (2)
C156	Public interests are important economic or financial interests of a Member State or of the European Union	30. (2)
C157	The economic or financial interests are monetary, budgetary or taxation matters	30. (2)
C158	Public interests are monitoring, inspection or regulatory functions	30. (2)
C159	Regulatory functions include temporary tasks	30. (2)
C160	The monitoring, inspection or regulatory functions are connected with the exercise of official authority in the special cases	30. (2)
C161	A person submits a request to that effect	31. (1)
C162	Data relate to the person	31. (1), 36. (1)
C163	The communication include the processed data	31. (1)
C164	The communication include the purposes of the processing	31. (1)
C165	The communication include the categories of recipients of the data	31. (1)
C166	The communication include any available information as to the source of such data	31. (1)
C167	The requests are about whether or not data is processed	31. (2)
C168	The request has not been replied to within 4 weeks from receipt of the request	31. (2)
C169	The information contains the grounds for the delay	31. (2)
C170	The information contains the time	31. (2)
C171	The decision can be expected to be available at the time	31. (2)
C172	Data are processed on behalf of the public administration in the course of its administrative procedures	32. (2)
C173	The rules of section 2, sections 7 to 11 and section 14 of the Act on Public Access to Documents in Administrative Files are applicable.	32. (2)
C174	Data are processed on behalf of the courts	32. (3)
C175	The data form part of a text	32. (3)
C176	The text is not available in its final form	32. (3)
C177	Data have been disclosed to a third party	32. (3)
C178	The access is to records of considerations of verdicts	32. (3)

(*continued on next page*)

(*continued*)

ID	Text	Source
C179	The access is to any other court records of the deliberations of the court	32. (3)
C180	The access is to material	32. (3)
C181	The material is prepared by the courts for the purpose of such deliberations	32. (3)
C182	Data are processed solely for scientific purposes	32. (4)
C183	Data are kept in personal form for a period	32. (4)
C184	The period does not exceed the other period	32. (4)
C185	The other period is necessary for the sole purpose of creating statistics	32. (4)
C186	The processing of data is in the area of criminal law	32. (5)
C187	The processing of data is carried out on behalf of the public administration	32. (5)
C188	The requests for rights of access in general are being turned down	32. (5)
C189	The data subject has received a communication	33.
C190	The data subject can establish that he has a specific interest to that effect	33.
C191	A new communication is 6 months after the last communication	33.
C192	The person has requested the form of the communication	34. (1)
C193	The communication is in a written form	34. (1)
C194	The interests of the data subject speak in favor thereof	34. (1)
C195	The communication is given in the form of oral information about the contents of the data	34. (1)
C196	The rules are given in writing by private companies	34. (2)
C197	The objection can be done at any time	35. (1)
C198	Data relate to the data subject	35. (1), 40.
C199	A data subject objects in relation to the controller to the processing of data	35. (2)
C200	The objection is justified	35. (2)
C201	A consumer objects	36. (1)
C202	Before a company discloses data to a third company	36. (2)
C203	Data concern a consumer	36. (2)
C204	The purposes of the disclose are marketing	36. (2)
C205	Before a company uses the data on behalf of a third company	36. (2)
C206	The purposes of the use are marketing	36. (2)
C207	The statement is to the effect that the consumer does not want to be contacted for the purpose of marketing activities	36. (2)
C208	The consumer has not given such information to the CPR-register	36. (2)
C209	The period of objection is two weeks	36. (2)
C210	The rules are issued by virtue of section 6 (7) of the Danish Marketing Act	36. (3)
C211	The communication is about the right to object	36. (3)
C212	Data turn out to be inaccurate	37. (1)
C213	Data turn out to be misleading	37. (1)
C214	Data turn out to be in any other way processed in violation of law or regulations	37. (1)
C215	A rectification, erasure or blocking carried out	37. (2)
C216	The notification proves impossible	37. (2)
C217	The notification involves a disproportionate effort	37. (2)
C218	The data subject objects	39. (1)
C219	The decision produces legal effects	39. (1)
C220	The effects concern the data subject	39. (1)
C221	The decision significantly affects the data subject	39. (1)
C222	The decision is based solely on automated processing of data	39. (1)
C223	The processing of data is intended to evaluate certain personal aspects	39. (1)
C224	The decision is taken in the course of the entering into or performance of a contract	39. (2)
C225	The request for the entering into or the performance of the contract has been satisfied	39. (2)
C226	The request is lodged by the data subject	39. (2)
C227	There are suitable measures to safeguard the legitimate interests of the data subject	39. (2)
C228	The decision is authorized by a law	39. (2)
C229	The law also lays down measures to safeguard the data subject's legitimate interests	39. (2)
C230	The controller makes the data subject to a decision	39. (3)
C231	The decisions is based on the rules	39. (3)
C232	The complaint concern the processing of data	40.
C233	A body performs work for the controller	41. (1)
C234	A body performs work for the processor	41. (1)
C235	A body has access to data	41. (1)
C236	It is provided by law or regulations	41. (1)
C237	Security measures are technical and organizational	41. (3)
C238	The data protection is against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in this Act	41. (3)
C239	Data are processed for the public administration	41. (4)
C240	Data are of special interest to foreign powers	41. (4)
C241	Measures are to ensure that data can be disposed of or destroyed in the event of war or similar conditions	41. (4)
C242	The rules concern the security measures	41. (5)
C243	The controller leaves the processing of data to a processor	42. (1), 42. (2)
C244	The contract must stipulate that the processor shall act only on instructions from the controller	42. (2)
C245	The contract must stipulate that the security measures are taken from the processor	42. (2)
C246	The notification is before processing of data is carried out on behalf of the public administration	43. (1)
C247	The notification must include the name and address of the controller and of his representative, if any, and of the processor, if any; the category of processing and its purpose; a general description of the processing; a description of the categories of data subjects and of the categories of data relating to them; the recipients or categories of recipients to whom the data may be disclosed; intended transfers of data to third countries; a general description of the measures taken to ensure security of processing; the date of the commencement of the processing; the date of erasure of the data	43. (2), 48. (2)

(*continued on next page*)

(*continued*)

ID	Text	Source
C248	Processing is of operations	44. (1)
C249	Operations do not cover data of a confidential nature	44. (1)
C250	The processing may include identification data	44. (1)
C251	The identification data include identification numbers	44. (1)
C252	The processing may include other data	44. (1)
C253	Other data concern payments to and from public authorities	44. (1)
_T11	it is a matter of processing as mentioned in section 45 (1).	44. (1)
C254	Processing is for the sole purpose of keeping a register	44. (3)
C255	The register according to law or regulations is intended to provide information to the public in general	44. (3)
C256	The register is open to public	44. (3)
_T12	processing includes data which are covered by section 7 (1) and section 8 (1);	45. (1)
C257	The processing of data includes alignment or combination of data for control purposes	45. (1)
C258	The rules include certain categories of processing of data that shall be exempt from the obligation of notification	44. (4)
C259	The rules include whether the opinion of the Agency shall be obtained prior to the start of any other processing operations	45. (2)
C260	Changes to the information may be notified at the latest 4 weeks after the implementation	46. (1), 46. (2)
C261	The processing of data include extra data from the Minister of Justice	46. (2)
C262	The data protection responsibility has been delegated to a subordinate authority	47. (1)
C263	The Data Protection Agency cannot approve the carrying out of a processing operation	47. (1)
C264	The Data Protection Agency cannot approve the carrying out of a processing operation on behalf of a municipal or county authority	47. (2)
C265	The notification is prior to the commencement of any processing of data	48. (1)
C266	Data is carried out on behalf of a private controller	48. (1)
C267	The processing of data relates to data about employees	49. (1)
_T13	Processing includes data as mentioned in section 8 (4)	49. (1)
C268	Data concern the health of employees	49. (1)
C269	The processing of health data is necessary to comply with provisions	49. (1)
C270	The provisions are laid down by law or regulations	49. (1)
C271	Data concern employees	49. (1)
C272	Registration is necessary under collective agreements or other agreements on the labor market	49. (1)
C273	Data concern customers, suppliers or other business relations	49. (1)
_T14	It is a matter of processing operations as mentioned in section 50 (1) 4	49. (1)
C274	The processing is carried out for the purpose of market surveys	49. (1)
C275	The processing is carried out by an association or similar body	49. (1)
C276	Data concern only the members of the association	49. (1)
C277	The processing is carried out by lawyers or accountants in the course of business	49. (1)
C278	Data concern only client matters	49. (1)
C279	The processing is carried out by doctors, nurses, dentists, dental technicians, chemists, therapists, chiropractors and other persons	49. (1)
C280	The other persons are authorized to exercise professional activities in the health sector	49. (1)
C281	Data are used solely for these activities	49. (1)
C282	The processing of the data is not carried out on behalf of a private hospital	49. (1)
C283	The processing is carried out for the purpose of being used by an occupational health service	49. (1)
C284	Rules are about other types of processing operations shall be exempt from the provisions	49. (3)
_T15	operations covered by section 50 (1)	49. (3)
_T16	the processing operations are exempted under section 50 (3)	
_T17	Prior to the commencement of any processing of data which is subject to the obligation to notify in section 48	50. (1)
C285	The processing of data is carried out for the purpose of warning third parties against entering into business relations	50. (1)
C286	The processing of data is carried out for the purpose of an employment relationship with a data subject	50. (1)
C287	The processing is carried out for the purpose of disclosure in the course of business of data for assessment of financial standing and creditworthiness	50. (1)
C288	The processing is carried out for the purpose of professional assistance in connection with staff recruitment	50. (1)
_T18	transfer of data as mentioned in subsection (1) to third countries by virtue of section 27 (1) and subsection (3) 2 to 4	
C289	The rules are to the effect that the authorization of the Agency shall be obtained prior to the commencement of other processing operations	50. (4)
C290	Other processing operations are subject to notifications	50. (4)
C291	The conditions are laid down when granting an authorization	50. (5)
C292	The conditions are for reasons of the protection of the privacy of the data subjects	50. (5)
C293	The notification is about changes in the information	51. (1)
C294	The notification is done prior to the changes being implemented	51. (1)
C295	The notification can be done at the latest 4 weeks after the implementation of the changes	51. (1)
_T19	operations covered by section 50 (1), (2) or (4).	
C296	The information is contained in notifications of processing operations	51. (2)
C297	Changes of the information are less important	51. (2)
C298	Processor is established in Denmark	53.
C299	Processor offers electronic processing services	53.
C300	The notification is done prior to the commencement of such processing operations	53.
C301	The operations are notified	54. (1)

(*continued on next page*)

(*continued*)

ID	Text	Source
C302	This register shall as a minimum contain the items of information	54. (1)
C303	The register shall be open to consultation by the general public	54. (1)
C304	The information concern the processing operations	54. (2)
C305	The processing operations are performed on the behalf of the controller	54. (2)
C306	The information includes the name and address of the controller and of his representative, if any, and of the processor, the category of processing and its purpose, a description of the categories of data subjects and of the categories of data relating to them, the recipients or categories of recipients to whom the data may be disclosed, intended transfers of data to third countries	54. (2)
C307	The restriction is necessary for the prevention, detection and prosecution of criminal offences	54. (3)
C308	The restriction is necessary because of essential considerations of private interests	54. (3)
C309	The Data Protection Agency consists of a Council and a Secretariat	55. (1)
C310	Operations are covered by this Act	55. (1)
C311	The data subject has given his explicit consent for the disclosing of data	8. (2)
C312	The processing operations are exempted by the Minister of Justice	49. (3)

A.2. Rights

The following table contains all the rights we have extracted from the data privacy regulations. Each right has a unique identifier (ID). The *stakeholder* is the actor, i.e. the person (or other object) that performs an *action* and this action is performed on an *object*. The constraints column includes a first-order logic that expresses the actual constraint. The *source* column includes where in the legal text this particular right is described. *Before* and *after* columns create a chain of rights and obligations, i.e. one should first consider the rights or/and obligations in the *before* field before applying the right. If there is no match with the right, the *after* field should be checked. Some parts of the legal text contain regions of type *see Section X*. We express this kind of relations in the *relation* column, i.e. one should check the right or/and obligation in this field along with the current right in the table.

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
R1	Common processor	may process	data	C4 & C5 & C6	5. (3)			
R2	Common processor	may process	personal data	C11 – (C12 & C13) – C14 – (C15 & C16) – C17 – (C18 & C19) – (C18 & (C20 & C21) – (C22 & C23)) – (C24 & (C25 – (C26 & C23)) & C27)	6. (1)			
R3	A company	may disclose	data to a third company	C28 & C29 & C31	6. (2)		O7	O9
R3.1	A company	may disclose	data to a third company	C28 & C29 & C34 & C35 & (C24 & (C25 – (C26 & C23)) & C27)	6. (3)	O7.1		
R4	A company	may use	data on behalf of a third company	C28 & C30 & C32	6. (2)		O8	O9
R4.1	A company	may use	data on behalf of a third company	C28 & C30 & C34 & C35 & (C24 & (C25 – (C26 & C23)) & C27)	6. (3)	O8.1		
R5	The Minister of Justice	may lay down	further restrictions in the access to disclose certain types of data	C28 & C29	6. (4)			
R6	The Minister of Justice	may lay down	further restrictions in the access to use certain types of data	C28 & C30	6. (4)			
R7	Common processor	may process	personal data	C11 – ((C38 & C40) – (C39 & C41)) – C42 – C43	7. (2)		O10	
R8	Common processor	may process	personal data	C44 & C45	7. (3)		O10	
R9	A non-profit-seeking body	may carry out	the processing of personal data in the course of its legitimate activities	C46 & ((C36 – C37) & (C47 – (C48 & C49)))	7. (4)			
R10	Common processor	may disclose	data	((C36 – C37) & (C47 – (C48 & C49))) & (C11 – (((C38 & C40) – (C39 & C41)) – C42 – C43 – (C44 & C45)))	7. (4)			
R11	Common processor	may process	personal data	(C36 – C37) & C50 & C51 & C52	7. (5)		O10	
R12	Common processor	may process	personal data	(C36 – C37) & C53	7. (6)		O10	
R13	The supervisory authority	may lay down	exemptions to the processing of personal data	(C36 – C37) & C54	7. (7)		O10	
R14	Common processor	may process	data on behalf of a public administration	(C57 & -(C36 – C37)) & C58	8. (1)		O14	
R15	Common processor	may disclose	data to a third party	(C57 & -(C36 – C37)) & C59 & (C311 – (C60 & C61) – (C62 – C63) – C64)	8. (2)		O15	

(*continued on next page*)

(*continued*)

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
R16	Administrative authorities	may disclose	data	C65 & ((C57 & -(C36 – C37)) – (C36 – C37)) & ((C311 – (C60 & C61)) – C66 – C67)	8. (3)			
R17	Private bodies	may process	data	(C57 & -(C36 – C37)) & (C11 – (C68 & C69))	8. (4)			
R18	Private persons	may process	data	(C57 & -(C36 – C37)) & (C11 – (C68 & C69))	8. (4)			
R19	Common processor	may disclose	data	(C57 & -(C36 – C37)) & C70 & C71	8. (5)		O16	
R20	Common processor	may process	data on behalf of a public administration	(C57 & -(C36 – C37)) & _T8	8. (6)		O14	
R21	Common processor	may disclose	data to a third party	(C57 & -(C36 – C37)) & C59 & _T8	8. (6)		O15	
R22	Private bodies	may process	data	(C57 & -(C36 – C37)) & _T8	8. (6)			
R23	Private persons	may process	data	(C57 & -(C36 – C37)) & _T8	8. (6)			
R24	Common processor	may disclose	data	(C57 & -(C36 – C37)) & _T8	8. (6)		O16	
R25	Common processor	may keep	a complete register of criminal convictions only under the control of a public authority		8. (7)			
R26	Common processor	may process	data	((C36 – C37) – C57) & C72 & C73	9. (1)			
R27	The supervisory authority	may lay down	specific conditions	((C36 – C37) – C57) & C72 & C73	9. (3)			
R28	The supervisory authority	may lay down	specific conditions	(C28 – C34 – C35 – C36 – C37 – C57) & C74	9. (3)			
R29	Common processor	may process	data	((C36 – C37) – C57) & C75 & C76	10. (1)			
R30	Common processor	may disclose	data to a third party	((C36 – C37) – C57) & C78	10. (3)			
R31	The supervisory authority	may lay down	specific conditions	((C36 – C37) – C57) & C78 & C79	10. (3)			
R32	Official authorities	may process	data	C80 & C81	11. (1)			
R33	Private bodies	may process	data	C80 & (C82 – C83 – C84)	11. (2)			
R33.1	Private bodies	may process	data	C80 & (C85 & ((C86 & C87) – C88))	11. (2)	O19		
R34	Private persons	may process	data	C80 & (C82 – C83 – C84)	11. (2)			
R34.1	Private persons	may process	data	C80 & (C85 & ((C86 & C87) – C88))	11. (2)	O19		
R35	Controller	may process	data	(C89 – C90) & (C91 – (C92 & C93) – C83)	12. (1)	O21		O20
R36	Public authority	may carry out	automatic registration of the telephone numbers	C94 & C96 & C97	13. (1)		O22	
R36.1	Public authority	may carry out	automatic registration of the telephone numbers	C94 & (C98 – (C99 & C100))	13. (2)		O22	
R37	Private company	may carry out	automatic registration of the telephone numbers	C95 & C96 & C97	13. (1)		O23	
R37.1	Private company	may carry out	automatic registration of the telephone numbers	C95 & (C98 – (C99 & C100))	13. (2)		O23	
R38	The supervisory authority	may lay down	specific conditions the automatic registration of the telephone numbers	C94 – C95	13. (1)			R36, R37, O22, O23
R39	Common processor	may archive	data under the rules	C101 & C102	14.			
R40	Common processor	may transfer	data to a third country	C103	27. (1)			O24
R41	Common processor	may transfer	data to a third country	C107 – C108 – (C109 & C110) – (C111 – C112) – C113 – C114 – C115 – (C116 & C117 & C118 & C119 & C120 & C121) – C122 – C123 – C124 – C125	27. (3)			
R42	The Data Protection Agency	may authorize	a transfer of personal data to a third country	C126 & -C103	27. (4)	R44		R40
R43	The Data Protection Agency	may lay down	specific conditions for the transfer of data to a third country		27. (4)			R42
R44	Common processor	may transfer	data to a third country	-C103 & C127 & C128	27. (5)		R42	
R45	Controller	shall not provide	the data subject with information	C129 & C130 & C131 & C132 & C133 & C134 & C138 & (C135 – C136 – C137) & C139	28. (2)		O26	
R46	Controller's representative	shall not provide	the data subject with information	C129 & C131 & C131 & C132 & C133 & C134 & C138 & (C135 – C136 – C137) & C139	28. (2)		O27	

(*continued on next page*)

(*continued*)

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
R47	Controller	shall not provide	the data subject with information	C140 & (C141 – C142) & C143 & C130 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137) & (C139 – C145)	29. (2)		O28	
R48	Controller's representative	shall not provide	the data subject with information	C140 & (C141 – C142) & C143 & C131 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137) & (C139 – C145)	29. (2)		O29	
R49	Controller	shall not provide	the data subject with information	C140 & (C141 – C142) & C143 & C130 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137) & (C146 – C147)	29. (3)		O28	
R50	Controller's representative	shall not provide	the data subject with information	C140 & (C141 – C142) & C143 & C131 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137) & (C146 – C147)	29. (3)		O29	
R51	Controller	shall not provide	the data subject with information	C129 & C130 & C131 & C132 & C133 & C134 & C138 & (C135 – C136 – C137) & C148 & C149	30. (1)		O26	
R52	Controller's representative	shall not provide	the data subject with information	C129 & C131 & C131 & C132 & C133 & C134 & C138 & (C135 – C136 – C137) & C148 & C149	30. (1)		O27	
R53	Controller	shall not provide	the data subject with information	C140 & (C141 – C142) & C143 & C130 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137) & C148 & C149	30. (1)		O28	
R54	Controller's representative	shall not provide	the data subject with information	C140 & (C141 – C142) & C143 & C131 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137) & C148 & C149	30. (1)		O29	
R55	Controller	shall not provide	the data subject with information	C129 & C130 & C131 & C132 & C133 & C134 & C138 & (C135 – C136 – C137) & (C150 & (C151 – C152 – C153 – C154 – C155 – (C156 & C57) – (C158 & C159 & C160 & (C153 – C154 – C155 – (C156 & C157)))))	30. (2)		O26	
R56	Controller's representative	shall not provide	the data subject with information	C129 & C131 & C131 & C132 & C133 & C134 & C138 & (C135 – C136 – C137) & (C150 & (C151 – C152 – C153 – C154 – C155 – (C156 & C57) – (C158 & C159 & C160 & (C153 – C154 – C155 – (C156 & C157)))))	30. (2)		O27	
R57	Controller	shall not provide	the data subject with information	C140 & (C141 – C142) & C143 & C130 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137) & (C150 & (C151 – C152 – C153 – C154 – C155 – (C156 & C57) – (C158 & C159 & C160 & (C153 – C154 – C155 – (C156 & C157)))))	30. (2)		O28	

(*continued on next page*)

(*continued*)

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
R58	Controller's representative	shall not provide	the data subject with information	C140 & (C141 – C142) & C143 & C131 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137) & (C150 & (C151 – C152 – C153 – C154 – C155 – (C156 & C57) – (C158 & C159 & C160 & (C153 – C154 – C155 – (C156 & C157)))))	30. (2)		O29	
R59	A body	may access	data	C174 & C175 & C176	32. (3)	O35	O34	
R60	Controller	shall not inform	the person whether or not data are being processed	C161 & C162 & (C182 – (C183 & C184 & C185))	32. (4)		O30	
R61	The Minister of Justice	may lay down	exemptions from the right of access	C161 & C162 & C186 & C187 &C188	32. (5)			
R62	Controller	shall not entitle	a data subject to a new communication	C161 & C162 & C189 & C191 & -C190	33.			
R63	Controller	may communicate	to the person	C161 & C162 & C194 & C195	34. (1)		O37	
R64	The Minister of Justice	may lay down	rules for payment for communications	C196	34. (2)			
R65	A data subject	may object	in relation to the controller to the processing of data	C197 & C198	35. (1)			
R66	Controller	shall not notify	the third party at the request of the data subject	C23 & C215 & (C212 – C213 – C214) & (C216 – C217)	37. (2)		O48	
R67	A data subject	may withdraw	his consent		38.			
R68	Controller	may make	the data subject to a decision	C218 & ((C219 & C220) – C221) & C222 & C223 & ((C224 & C225 & C226) – C227 – (C228 & C229))	39. (2)		O49	
R69	A data subject	has the right to be informed	by the controller as soon as possible and without undue delay about the rules	C231 & C230 & ((C219 & C220) – C221) & C222 & C223	39. (3)			R51-R58
R70	A data subject	may file	a complaint to the appropriate supervisory authority	C232 & C198	40.			
R71	A body	may process	data only on instructions from the controller	(C233 – C234) & C235	41. (1)		O50	
R72	The Minister of Justice	may lay down	more detailed rules	C242 & C237	41. (5)			O53, O54
R73	Controller	may authorize	other authorities or private bodies to make a notifications on his behalf	C246 & C247	43. (1), 43. (2)			
R74	Controller	shall not notify	the Data Protection Agency	C246 & C247 & C248 & C249 & ((C250 & C251) – (C252 & C253))	44. (1)	O61	O59	
R75	Controller's representative	shall not notify	the Data Protection Agency	C246 & C247 & C248 & C249 & ((C250 & C251) – (C252 & C253))	44. (1)	O61	O60	
R76	Controller	may process	data	C248 & C249 & ((C250 & C251) – (C252 & C253))	44. (1)	O62		
R77	Controller's representative	may process	data	C248 & C249 & ((C250 & C251) – (C252 & C253))	44. (1)	O63		
R78	Controller	shall not notify	the Data Protection Agency	C254 & C255 & C256	44. (3)		O59	
R79	Controller's representative	shall not notify	the Data Protection Agency	C254 & C255 & C256	44. (3)		O60	
R80	The Minister of Justice	may lay down	rules	C258	44. (4)			O59, O60
R81	The Minister of Justice	may lay down	rules	C259	45. (2)			
R82	Common processor	may notify	less important changes to the information to the Data Protection Agency subsequently	((C36 – C37 – C57) – C74 – C84 – C257) & C260	46. (1)			
R83	Controller	must not notify	the Data Protection Agency	C265 & C266 & (((C267 – C274 – C273) & -((C57 & -(C36 – C37)) – (C36 – C37))) – (C268 & C269 & C270) – (C271 & C272) – (C273 & -288) – (C275 & C276) – (C277 & C278) – (C279 & C280 & C281 & C282) – C283)	49. (1)	O77	O73	

(*continued on next page*)

(*continued*)

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
R84	The Minister of Justice	may lay down	rules	C284	49. (3)			O73
R85	The Minister of Justice	may lay down	exemptions from the provisions	((C265 & C266) & ((C36 – C37) – (C57 & -(C36 – C37)))) – ((C265 & C266) & (C103 – C108 – (C109 & C110) – (C111 – C112) – C113 – C114))	50. (3)			
R86	The Minister of Justice	may lay down	rules	C289 & C290	50. (4)			O76, O77
R87	The Data Protection Agency	may lay down	specific conditions for the carrying out of the processing operations	C291 & C292	50. (5)			O76, O77, R86
R88	Common processor	may notify	the Data Protection Agency subsequently	C293 & C247 & C295	51. (1)			
R89	The supervisory authority	may restrict	the right of access of the general public to the register	C307 – C308	54. (3)			O82
R90	The supervisory authority	may restrict	the right of access of the general public to the information	C306 & (C307 – C308)	54. (3)			

A.3. Obligations

The following table contains all the obligations we have extracted from the data privacy regulations. Each obligation has a unique identifier (ID). The *stakeholder* is the actor, i.e. the person (or other object) that performs an *action* and this action is performed on an *object*. The constraints column includes a first-order logic that expresses the actual constraint. The *source* column includes details about where in the legal text a particular obligation is described. *Before* and *after* columns create a chain of rights and obligations, i.e. one should first consider the rights/obligations in the *before* field before applying the obligation from the row. If

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
O1	Common processor	must process	data in accordance with good practices for processing data		5. (1)			
O2	Common processor	must collect	data for purposes	C1 & C2 & C3	5. (2)			
O3	Common processor	must organize	the processing of data in a way	C7	5. (4)			
O4	Common processor	must make	necessary checks	C8	5. (4)			
O5	Common processor	must erase / rectify	data	C9	5. (4)			
O6	Common processor	may not keep	the collected data in a form	C10	5. (5)			
O7	A company	may not disclose	data to a third company	C28 & C29	6. (2)	R3		
O7.1	A company	may not disclose	data to a third company	C36 – C37 – C57	6. (4)		R3.1	
O8	A company	may not use	data on behalf of a third company	C28 & C30	6. (2)	R4		
O8.1	A company	may not use	data on behalf of a third company	C36 – C37 – C57	6. (4)		R4.1	
O9	A company	shall obtain	the consent in accordance with the rules	C33	6. (2)			
O10	Common processor	may not process	personal data	C36 – C37	7. (1)	R7, R8, R11, R12, R13		
O11	The supervisory authority	shall give	its authorization for the exemptions of processing personal data	(C36 – C37) & C54	7. (7)			R13
O12	The supervisory authority	shall notify	the Commission of any derogation of the processing of personal data	(C36 – C37) & C54	7. (7)			
O13	Common processor	may not keep	automatic registers on behalf of a public administration	C55 & C56	7. (8)			
O14	Common processor	may not process	data on behalf of a public administration	C57 & -(C36 – C37)	8. (1)	R14, R20		
O15	Common processor	may not disclose	data to a third party	C59	8. (2)	R15, R21		
O16	Common processor	may not disclose	data	(C57 & -(C36 – C37)) & -C11	8. (5)	R19, R24		
O17	Common processor	may not process	data subsequently	((C36 – C37) – C57 – C74) & -(C72 & C73)	9. (2)			R2, R3, R3.1, R4, R4.1, R5, R6, O7, O7.1, O8, O8.1

(*continued on next page*)

(*continued*)

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
O18	Common processor	may not process	data subsequently	((C36 – C37) – C57 – C77) & -(C75 & C76)	10. (2)			R2, R3, R3.1, R4, R4.1, R5, R6, O7, O7.1, O8, O8.1
O19	Common processor	may not make	public an identification number	C80 & -C83	11. (3)		R33.1, R34.1	
O20	Controller	shall obtain	the consent in accordance with the rules	(C89 – C90) & C33	12. (1)			R35
O21	Controller	may not process	data	(C89 – C90) & ((C36 – C37) – C57)	12. (2)		R35	
O22	Public authority	may not carry out	any automatic registration of the telephone numbers	C94	13. (1)	R36, R36.1		
O23	Private company	may not carry out	any automatic registration of the telephone numbers	C95	13. (1)	R37, R37.1		
O24	Common processor	shall assess	the adequacy of the level of protection in the light of all the circumstances	C104 & C105 & C106	27. (2)			
O25	The Data Protection Agency	shall inform	the European Commission and the other Member States of the authorizations granted pursuant		27. (4)			R42
O26	Controller	shall provide	the data subject with information	C129 & C130 & C131 & C132 & C133 & C134 & C138 & (C135 – C136 – C137)	28. (1)	R45, R51, R55		
O27	Controller's representative	shall provide	the data subject with information	C129 & C131 & C131 & C132 & C133 & C134 & C138 & (C135 – C136 – C137)	28. (1)	R46, R52, R56		
O28	Controller	shall provide	the data subject with information	C140 & (C141 – C142) & C143 & C130 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137)	29. (1)	R47, R49, R53, R57		
O29	Controller's representative	shall provide	the data subject with information	C140 & (C141 – C142) & C143 & C131 & C131 & C132 & C133 & C134 & C138 & (C144 – C135 – C136 – C137)	29. (1)	R48, R50, R54, R58		
O30	Controller	shall inform	the person whether or not data are being processed	C161 & C162	31. (1)	R60		
O31	Controller	shall communicate	to the person	C162 & (C163 & C164 & C165 & C166)	31. (1)			
O32	Controller	shall reply	to requests without delay	C167 & C162	31. (2)			
O33	Controller	shall inform	the person in question	C168 & C169 & C170 & C171	31. (2)			
O34	A body	may not access	data	C172 & C173	32. (2)	R59		
O35	A body	may not access	data	C174 & C175 & C176 & C177	32. (2)		R59	
O36	A body	has no right	of access	C178 – C179 – (C180 & C181)	32. (3)			
O37	Controller	shall communicate	to the person	C161 & C162 & C192 & C193	34. (1)	R63		
O38	Controller	may not involve	data in the processing	C199 & C198 & C200	35. (2)			
O39	A company	may not disclose	data to a third company	C201 & C162 & C29	36. (1)			
O40	A company	may not use	data on behalf of a third company	C201 & C162 & C30	36. (1)			
O41	A company	must check	the CPR-register whether the consumer has filed a statement	C203 & ((C202 & C204) – (C205 & C206)) & C207	36. (2)			
O42	A company	shall provide	information about the right to object in a clear and intelligible manner	C203 & ((C202 & C204) – (C205 & C206)) & C208	36. (2)			
O43	A company	shall give	access to the consumer to object in a simple manner	C203 & ((C202 & C204) – (C205 & C206)) & C208 & C209	36. (2)			
O44	A company	may not disclose	data until the time limit has expired	C203 & ((C202 & C204) – (C205 & C206)) & C208 & C209	36. (2)			

(*continued on next page*)

(*continued*)

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
O45	A company	shall contact	the consumer in accordance with the rules	C33 & C210 & C211	36. (3)			O42
O46	A company	may not demand	any payment of fees in connection with objections		36. (4)			
O47	Controller	shall rectify, erase or block	data at the request of the data subject	C212 – C213 – C214	37. (1)			
O48	Controller	shall notify	the third party at the request of the data subject	C23 & C215 & (C212 – C213 – C214)	37. (2)	R66		
O49	Controller	may not make	the data subject subject to a decision	C218 & ((C219 & C220) – C221) & C222 & C223	39. (1)	R68		
O50	A body	may not process	data only on instructions from the controller	(C233 – C234) & C235 & C236	41. (1)	R71		
O51	Controller	may not restrict	journalistic freedom with the instructions	(C233 – C234) & C235	41. (2)			R71
O52	Controller	may not impede	the production of an artistic or literary product with the instructions	(C233 – C234) & C235	41. (2)			R71
O53	Controller	shall implement	appropriate security measures to protect data	C237 & C238	41. (3)			
O54	Processor	shall implement	appropriate security measures to protect data	C237 & C238	41. (3)			
O55	Common processor	shall take	measures	C239 & C240 & C241	41. (4)			
O56	Controller	shall make sure	that the processor is in a position to implement the security measures	C243 & C237	42. (1)			O53, O54, R72
O57	Controller	shall ensure	that the processor comply with the security measures	C243 & C237	42. (1)			O53, O54, R72
O58	Controller	shall sign	a written contract with the processor	C243 & C244 & C245 & C237 & C238 & ((C239 & C240) – C241)	42. (2)			
O59	Controller	shall notify	the Data Protection Agency	C246 & C247	43. (1), 43. (2)	R74, R78		
O60	Controller's representative	shall notify	the Data Protection Agency	C246 & C247	43. (1), 43. (2)	R75, R79		
O61	The Minister of Justice	shall lay down	more detailed rules on the processing operations	C249	44. (1)		O74, O75	
O62	Controller	shall notify	the Data Protection Agency	C248 & C249 & ((C36 – C37 – C57) – C74 – C84 – C257)	44. (1)		R76	
O63	Controller's representative	shall notify	the Data Protection Agency	C248 & C249 & ((C36 – C37 – C57) – C74 – C84 – C257)	44. (1)		R77	
O64	Common processor	must obtain	the opinion of the Data Protection Agency	C246 & ((C36 – C37 – C57) – C74 – C84 – C257)	45. (1)			
O65	The Minister of Justice	may not lay down	rules	C258 & ((C36 – C37 – C57) – C74 – C84 – C257)	44. (4)			O59, O60
O66	Common processor	shall notify	changes to the information to the Data Protection Agency prior to being implemented	(C36 – C37 – C57) – C74 – C84 – C257	46. (1)			
O67	Common processor	shall obtain	the opinion of the Data Protection Agency prior to the implementation of changes in the information	(C36 – C37 – C57) – C74 – C84 – C257 – C261	46. (2)			
O68	Common processor	shall notify	less important changes in the information to the Data Protection Agency	((C36 – C37 – C57) – C74 – C84 – C257 – C261) & C260	46. (2)			
O69	The Data Protection Agency	shall bring	the matter before the competent Minister	C262 & C263	47. (1)			O70
O70	A competent Minister	shall decide	the matter	C262 & C263	47. (1)			
O71	The Data Protection Agency	shall bring	the matter before the Minister of the Interior	C264	47. (2)			O72
O72	The Minister of Interior	shall decide	the matter	C264	47. (2)			
O73	Controller	must notify	the Data Protection Agency	C265 & C266 & C247	48. (1), 48. (2)	R83		
O74	The Minister of Justice	shall lay down	more detailed rules		49. (2)			R83

(*continued on next page*)

(*continued*)

ID	Stakeholder	Action	Object	Constraints	Source	Before	After	Relation
O75	The Minister of Justice	may not lay down	rules	C284 & (((C36 – C37) – (C57 & -(C36 – C37))) – (C285 – C286) – C287 – C288 – C74) & -C312	49. (3)			R85
O76	Common processor	must obtain	the authorization of the Data Protection Agency	(C265 & C266) & (((C36 – C37) – (C57 & -(C36 – C37))) – (C285 – C286) – C287 – C288 – C74)	50. (1)			
O77	Common processor	must obtain	the authorization of the Data Protection Agency to a transfer	(C103 – C108 – (C109 & C110) – (C111 – C112) – C113 – C114) & (C265 & C266)	50. (2)		R83	
O78	Common processor	must notify	the Data Protection Agency	C293 & C294 & C247	51. (1)			
O79	Common processor	shall obtain	the authorization of the Data Protection Agency	(((C36 – C37) – (C57 & -(C36 – C37))) – (C285 – C286) – C287 – C288 – C74) & C296 & C247	51. (2)			
O80	Common processor	shall notify	the Data Protection Agency	(((C36 – C37) – (C57 & -(C36 – C37))) – (C285 – C286) – C287 – C288 – C74) & C296 & C247 & C297 & C295	51. (2)			
O81	Processor	must notify	the Data Protection Agency	C298 & C299 & C300	53.			
O82	The supervisory authority	shall keep	a register of processing operations	C301 & (C302 & C247) & C303 & (C246 – C266)	54. (1)			
O83	Controller	must make	the information available to any person	C304 & C305 & C306	54. (2)			
O84	The Data Protection Agency	is responsible for	supervision of all processing operations	C309 & C310	55. (1)			

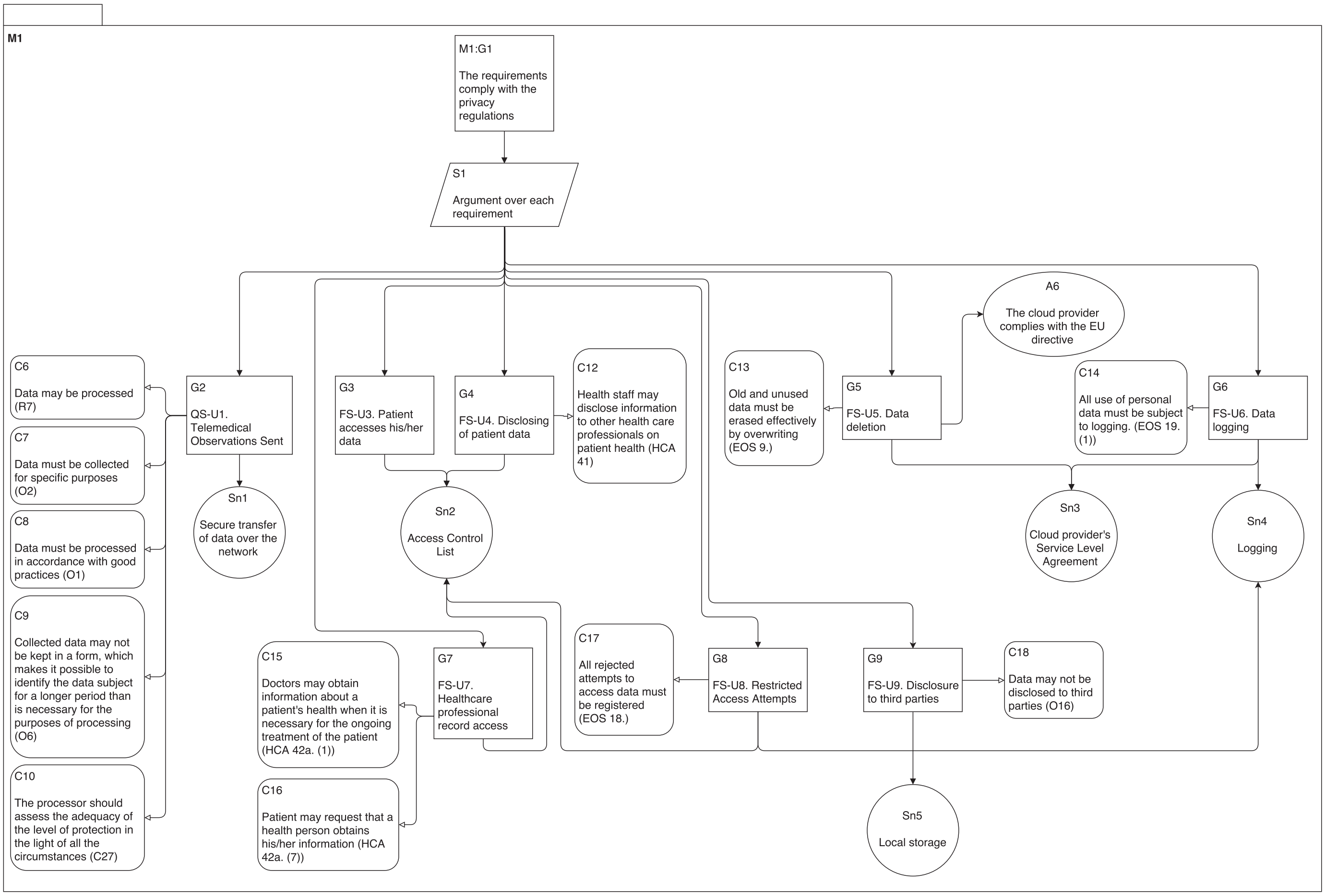
M1
M1:G1
The requirements comply with the privacy regulations
S1
Argument over each requirement
A6
The cloud provider complies with the EU directive
C6
Data may be processed (R7)
C7
Data must be collected for specific purposes (O2)
C8
Data must be processed in accordance with good practices (O1)
C9
Collected data may not be kept in a form, which makes it possible to identify the data subject for a longer period than is necessary for the purposes of processing (O6)
C10
The processor should assess the adequacy of the level of protection in the light of all the circumstances (C27)
G2
QS-U1. Telemedical Observations Sent
Sn1
Secure transfer of data over the network
G3
FS-U3. Patient accesses his/her data
G4
FS-U4. Disclosing of patient data
C12
Health staff may disclose information to other health care professionals on patient health (HCA 41)
Sn2
Access Control List
C13
Old and unused data must be erased effectively by overwriting (EOS 9.)
G5
FS-U5. Data deletion
C14
All use of personal data must be subject to logging. (EOS 19. (1))
G6
FS-U6. Data logging
Sn3
Cloud provider's Service Level Agreement
Sn4
Logging
C15
Doctors may obtain information about a patient's health when it is necessary for the ongoing treatment of the patient (HCA 42a. (1))
C16
Patient may request that a health person obtains his/her information (HCA 42a. (7))
G7
FS-U7. Healthcare professional record access
C17
All rejected attempts to access data must be registered (EOS 18.)
G8
FS-U8. Restricted Access Attempts
G9
FS-U9. Disclosure to third parties
C18
Data may not be disclosed to third parties (O16)
Sn5
Local storage

Fig. B.7. GSN argument for correctness – full model.

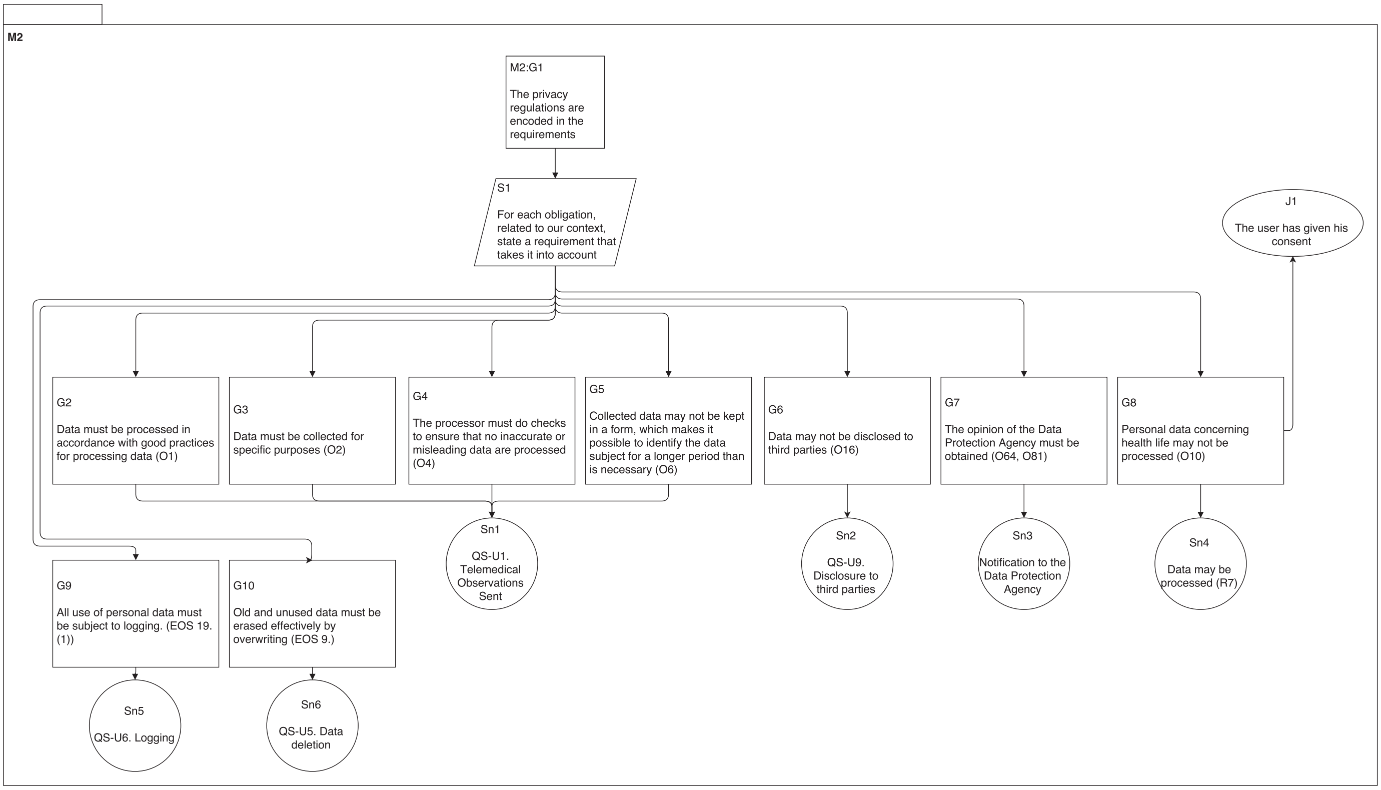
M2
M2:G1
The privacy regulations are encoded in the requirements
S1
For each obligation, related to our context, state a requirement that takes it into account
J1
The user has given his consent
G2
Data must be processed in accordance with good practices for processing data (O1)
G3
Data must be collected for specific purposes (O2)
G4
The processor must do checks to ensure that no inaccurate or misleading data are processed (O4)
G5
Collected data may not be kept in a form, which makes it possible to identify the data subject for a longer period than is necessary (O6)
G6
Data may not be disclosed to third parties (O16)
G7
The opinion of the Data Protection Agency must be obtained (O64, O81)
G8
Personal data concerning health life may not be processed (O10)
Sn1
QS-U1. Telemedical Observations Sent
Sn2
QS-U9. Disclosure to third parties
Sn3
Notification to the Data Protection Agency
Sn4
Data may be processed (R7)
G9
All use of personal data must be subject to logging. (EOS 19. (1))
G10
Old and unused data must be erased effectively by overwriting (EOS 9.)
Sn5
QS-U6. Logging
Sn6
QS-U5. Data deletion

Fig. B.8. GSN argument for completeness – full model.

there is no match with the obligation, the *after* field should be checked. Some parts of the legal text contain regions of type *see Section X*. We express this kind of relations in the *relation* column, i.e. one should check the rights/obligations in this field along with the current obligation in the table.

Appendix B. GSN model

The full GSN models are presented – the one for correctness and the one for completeness.

References

Attwood, K., Chinneck, P., Clarke, M., Cleland, G., Coates, M., Cockram, T., Despotou, G., Emmet, L., Fenn, J., Gorry, B., Habli, I., Hall, C., Harrison, A., Hawkins, R., Hutchison, P., Jackson, A., Kelly, T., Littlejohns, P., Mayo, P., Logan, L., Pierce, R., Pygott, C., Scott, G., Warren, M., Williams, P., 2011. GSN Community Standard Version 1. The GSN Working Group.

Bass, L., Clements, P., Kazmann, R., 2012. Software Architecture in Practice, 3rd ed Addisson-Wesley.

Breaux, T.D., Antón, A.I., 2008. Analyzing regulatory rules for privacy and security requirements. IEEE Trans. Softw. Eng. 34 (1), 5–20.

Breaux, T.D., Gordon, D.G., 2013. Regulatory requirements traceability and analysis using semi-formal specifications. In: Requirements Engineering: Foundation for Software Quality. Springer, pp. 141–157.

Breaux, T.D., Vail, M.W., Antón, A.I., 2006. Towards regulatory compliance: extracting rights and obligations to align requirements with regulations. In: Requirements Engineering, 14th IEEE International Conference. IEEE, pp. 49–58.

Christensen, H.B., Hansen, K.M., Kyng, M., Manikas, K., 2014. Analysis and design of software ecosystem architectures – towards the 4s telemedicine ecosystem. Inf. Softw. Technol. 56 (11), 1476–1492. doi:10.1016/j.infsof.2014.05.002.Special issue on Software Ecosystems URL http://www.sciencedirect.com/science/article/pii/S0950584914001050.

Datatilsynet, 2011a. Guidance to executive order on security. http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/guidance-to-executive-order-on-security/. Accessed on 2014-mar-8.

Datatilsynet, 2011b. Processing of sensitive personal data in a cloud solution. http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/. Accessed on 2014-mar-8.

Datatilsynet, 2013. The act on processing of personal data. http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/.

Digitaliseringsstyrelsen, 2012. Cloud computing and the legal framework (in danish). http://www.digst.dk/Arkitektur-og-standarder/Cloud-computing/De-juridiske-rammer.

European Commission, 1993. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices. Official Journal L 169, 12/07/1993 P. 0001 - 0043.

European Commission, 2012a. How will the EU's reform adapt data protection rules to new technological developments? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf. Accessed on 2015-03-13.

European Commission, 2012b. Proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. COM(2012) 11 final.

European Parliament and the Council of The European Union, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

European Union, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

European Union Agency for Network and Information Security, 2009. Cloud computing. benefits, risks and recommendations for information security. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/.

FDA, 2013. Personal Genonme Service (PGS). Warning letter. http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm376296.htm.

FDA, 2014. Title 21 – Food and Drugs. Chapter 1 – Food and Drug Administration. Subchapter H – Medical Devices. Part 820 Quality System Regulation. US Food and Drug Administration.

Ghanavati, S., Amyot, D., Peyton, L., 2007. Towards a framework for tracking legal compliance in healthcare. In: Advanced Information Systems Engineering. Springer, pp. 218–232.

Glaser, B.G., Strauss, A.L., 1967. The discovery of grounded theory: strategies for qualitative research. Aldine de Gruyter.

Graydon, P., Habli, I., Hawkins, R., Kelly, T., Knight, J., 2012. Arguing conformance. IEEE Softw. 29 (3), 50–57.

He, Y., Johnson, C., 2012. Generic security cases for information system security in healthcare systems. IET Conference Proceedings.URL http://digital-library.theiet.org/content/conferences/10.1049/cp.2012.1507.

IEC, 2002. Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS). 1.0 edition. International Standard IEC 62278.

Indenrigs- og Sundhedsministeriet, 2010. Sundhedsloven, LBK nr 913. https://www.retsinformation.dk/Forms/r0710.aspx?id=130455. Accessed on 2014-mar-11.

Islam, S., 2009. Software development risk management model: a goal driven approach. In: Proceedings of the Doctoral Symposium for ESEC/FSE on Doctoral Symposium. ACM, pp. 5–8.

Islam, S., Mouratidis, H., Jürjens, J., 2011. A framework to support alignment of secure software engineering with legal regulations. Softw. Syst. Model. 10 (3), 369–394.

Islam, S., Mouratidis, H., Wagner, S., 2010. Towards a framework to elicit and manage security and privacy requirements from laws and regulations. In: Requirements Engineering: Foundation for Software Quality. Springer, pp. 255–261.

ISO/IEC, 1998-2000. Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems. 1st edition. International Standard ISO/IEC 61508, Parts 1-7.

Kelly, T., Weaver, R., 2004. The goal structuring notation – a safety argument notation. In: Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, p. 6.

Kiyavitskaya, N., Zeni, N., Breaux, T.D., Antón, A.I., Cordy, J.R., Mich, L., Mylopoulos, J., 2007. Extracting rights and obligations from regulations: toward a tool-supported process. In: Proceedings of the Twenty-Second IEEE/ACM International Conference on Automated Software Engineering. ACM, pp. 429–432.

Manikas, K., Hansen, K.M., Kyng, M., 2014. Governance mechanisms for healthcare apps. In: Proceedings of the 2014 European Conference on Software Architecture Workshops. ACM, p. 10.

Mihaylov, B., Onea, L., 2013. Towards a Cloud-based Architecture for Telemedicine. University of Copenhagen.

Net4Care, 2012. The Net4Care Platform – Version 0.3.

Sujan, M.-A., Koornneef, F., Voges, U., 2007. Goal-based safety cases for medical devices: opportunities and challenges. In: Saglietti, F., Oster, N. (Eds.), Computer Safety, Reliability, and Security. In: Lecture Notes in Computer Science, 4680. Springer Berlin Heidelberg, pp. 14–27. URL http://dx.doi.org/10.1007/978-3-540-75101-4_2.

Sundhedsstyrelsen, 2013. Bekendtgørelse om autoriserede sundhedspersoners patientjournaler. https://www.retsinformation.dk/Forms/r0710.aspx?id=144978. Accessed on 2014-mar-1.

Thomson Reuters, 2015. Cost of compliance 2015. https://risk.thomsonreuters.com/sites/default/files/GRC02332.pdf.

United States Congress, 1996. The Health Insurance Portability and Accountability Act of 1996. http://legislink.org/us/pl-104-191.

U.S. Department of Health and Human Services – Food and Drug Administration, 2013. Mobile medical applications – guidance for industry and food and drug administration staff. http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf.

U.S. Environmental Protection Agency, 2015. EPA, California Notify Volkswagen of Clean Air Act Violations / Carmaker allegedly used software that circumvents emissions testing for certain air pollutants. http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/dfc8e33b5ab162b985257ec40057813b!opendocument.

VI MARGRETHE DEN ANDEN, 2013. Lov om offentlighed i forvaltningen. https://www.retsinformation.dk/Forms/r0710.aspx?id=152299. Accessed on 2014-mar-1.

Vivas, J., Agudo, I., López, J., 2011. A methodology for security assurance-driven system development. Req. Eng. 16 (1), 55–73. doi:10.1007/s00766-010-0114-8.URL http://dx.doi.org/10.1007/s00766-010-0114-8.

Boyan Mihaylov is a software architect at UniPension, Denmark. He received his M.Sc. degree from University of Copenhagen in 2013.

Lucian Onea is a software developer at Endomondo. He received his M.Sc.degree from University of Copenhagen in 2013.

Klaus Marius Hansen is a full professor (on leave) of Computer Science at University of Copenhagen. He received his Ph.D. from Aarhus University in 2002.