Operationalization of privacy and security requirements for eHealth IoT applications in the context of GDPR and CSL

Oleksandr Tomashchuk^{1,3} *, Yuan Li² *, Dimitri Van Landuyt³, and Wouter Joosen³

¹ Philips Research, Eindhoven, Netherlands, oleksandr.tomashchuk@philips.com

² University of Macerata, Macerata, Italy, y.li6@studenti.unimc.it

³ imec-DistriNet, KU Leuven, Heverlee, Belgium,
{[dimitri.vanlanduyt](mailto:dimitri.vanlanduyt@kuleuven.be),[wouter.joosen](mailto:wouter.joosen@kuleuven.be)}@kuleuven.be

Abstract. The Fourth Industrial Revolution imposes a number of unprecedented societal challenges and these are increasingly being addressed through regulation. This, in turn, lays the burden to adopt and implement the different concepts and principles (such as privacy-by-design) with practitioners. However, these concepts and principles are formulated by legal experts in a way that does not allow their direct usage by software engineers and developers, and the practical implications are thus not always obvious nor clear-cut. Furthermore, many complementary regulatory frameworks exist to which compliance should, in some cases, be reached simultaneously.

In this paper, we address this generic problem by transforming the legal requirements imposed by the EU’s General Data Protection Regulation (GDPR) and the China’s Cybersecurity Law (CSL) into technical requirements for an exemplar case study of a generic eHealth IoT system. The derived requirements result from an interdisciplinary collaboration between technical and legal experts and are representative of the types of trade-off decisions made in such a compliance process. By means of this exemplar case study, we propose a set of generic requirement-driven elements that can be applied to similar IoT-based architectures and thereby reduce the role of supervision from a legal point of view in the development of such architectures.

Keywords: IoT · eHealth · GDPR · CSL · Requirements.

1 Introduction

The widespread proliferation of Internet-of-Things (IoT) raises a number of non-trivial societal challenges. IoT devices are embedded in the physical surroundings of human beings, and IoT-based applications in many cases are used to manage systems that directly affect human actors, e.g. in a smart home, smart city or

* The authors contributed equally.

smart traffic context. The common characteristics of such systems is that they systematically gather personal data in a continuous and fine-grained fashion, and thus they impose non-trivial risks to the fundamental privacy rights of involved data subjects.

The latter is especially true in the case of IoT-based health applications, which deal with health indicators, information related to physical state, the whereabouts and activities of individual patients. In the HEART project [1], we focus on a number of specific application cases driven by IoT. Some examples involve (i) sleep description analysis, (ii) gestational weight gain prediction, (iii) recommender system for pregnancy application. Each eHealth application case involves its own intrinsic design challenges, and given the nature of the involved data, these systems impose even more substantial risks to fundamental privacy rights.

Modern data processing activities efficiently leverage the massive amounts of computational power available in today's systems, and activities involving the large-scale collection (such as IoT) and Big Data analytics by design involve large amounts of personal data. To deal with the challenges and risks raised by these evolutions in technology, several Legislative and Regulatory efforts have emerged. In the context of the European Union (EU), the well-known General Data Protection Regulation (GDPR) has come into force in 2018. Similarly, in the context of China, the Cybersecurity Law (CSL) has established a number of fundamental rights related to the processing of personal information.

In contemporary development practices, the development of software-intensive systems and service is seldom restricted to a single geographical location. Furthermore, if different regulatory constraints are not explicitly taken into account, there is a significant risk that the created services will only be applicable within a single geographical area of application. The initial investment costs of compliance analysis vis-a-vis different regulations thus will drastically pay off if the created products and services will be viable across different markets.

The existing state-of-the-art offers some research towards operationalization of the GDPR and other legislations. For example, Hintze and LaFever [17] tried to elaborate on GDPR requirements. However, they focused on the concept of Controlled Linkable Data, which does not fully cover the broad variety of technical requirements that arise from the GDPR. Also, Brodin [9] introduced a framework for GDPR compliance for SMEs, but the influence of GDPR requirements on solutions architecture is not adequately highlighted by this work. Ayala-Rivera and Pasquale [6] tried to operationalize the GDPR requirements by proposing a 6-step approach for elicitation of requirements, although they did not propose the requirements themselves. A similar situation can be observed in [12]. Some requirements were extracted from the recitals and articles of the GDPR in [18], [5], [31] and [25], but the authors did not study the influence of obtained requirements on architectures. Furthermore, there were some trials for investigation on geographical implications ([11], [16], [29], [14], [5]), however, the authors did not extract the requirements and did not demonstrate their implications on architectures.

Problem statement. The regulations establish core principles, to which compliance must be attained and demonstrated. However, there is a large distance between these principles and requirements that are understandable and can be addressed by software engineers in the development life-cycle of these systems. Commercial cooperations in the eHealth sector between the European Union and China that are rooted in completely different legal, cultural, and academic backgrounds can create new challenges: (i) operationalization of the principles and thus requirements is non-trivial and demands extensive expertise, and (ii) when dealing with solutions that are to be rolled out across multiple geographical locations, specific expertise is required on each applicable legislations.

Approach. In this paper, we address the identified problem through an *exemplar* eHealth case study. This is an abstracted system architecture that exhibits the most prominent characteristics of the eHealth system described above. We first discuss and compare the main implications of both the GDPR and the CSL in this specific context, and then we translate the implications into technical Privacy and Security requirements. Application of the latter is firstly investigated on simplified architecture (entities are limited to a human user, a database, and a stakeholder), and then spread to an extracted from the state-of-the-art reference eHealth IoT architecture.

The remainder of the paper is structured as follows: Section 2 provides an overview of the GDPR and the CSL and discusses commonalities and differences between them. Section 3 demonstrates the influence of GDPR and CSL requirements on architectures, and Section 4 concludes the paper and highlights future work.

2 A comparison of the GDPR and the CSL: two sides of the coin?

One impression about China is that it is like a privacy-vacuum territory where no data protection rules have been implemented. It is not the case until China released its Cybersecurity Law in 2015, six months after the GDPR was well known globally. This legislation slipped away under the radar due to its competence being limited inside the territory of the People’s Republic of China, but its importance should not be undermined. This section outlines the core requirements of the GDPR and the CSL on personal information protection. It aims at providing legal implications for further technical interpretations.

The CSL is the highest-level standard framework on personal information protection in China. It is broader than the GDPR. The objectives are to govern everything within the country’s digital infrastructure, from cyberspace information regulation to the data export. This legislation is an evolving project that is still being worked on by competent authorities such as the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), together with active interactions among industrial entities.

As its name suggests, the CSL is mainly devoted to provisions involving the security of cyberspace networks. A special category of security procedures and requirements is mandated for the “critical information infrastructure operators” i.e. energy, transportation or public services sectors.⁴ Except where these topics touch on personal information protection, they are not the subject of this article.

Due to certain commonalities laying between the GDPR and the CSL, it is easy to classify the two as similar frameworks at first glance. Scholars considered the CSL having been modelled based on the GDPR, or even claimed it as the “Chinese version of the GDPR” [32]. However, the provisions of the two laws are inconsistent, thus leading to different requirements for legal compliance. We reasoned this as follows.

2.1 GDPR and CSL: an overview

The GDPR highlights the principle of the supremacy of data privacy by (i) greatly expanding the scope and protection mechanisms of data subjects’ rights; (ii) significantly regulating the processing of personal data by data controllers and processors and; (iii) increasing the controllers’ legal responsibilities for personal data management. The GDPR also clarifies some exceptions based on highlighting the private protection of personal data. When private rights conflict with public rights, public rights take precedence. For example, when the rights and principles of personal data protection conflict with national security, government surveillance, public security, public interest or judicial procedures, the needs of the latter should be met first.

The CSL’s provisions relating to data privacy formed what China’s most comprehensive and broadly applicable set of data privacy rules to date are. These provisions implanted many of the basic principles and requirements that can be found in other laws and regulations. However, its set of data protection provisions is extensive, including numerous normative texts scattered across various industries (such as the Administrative Measures for e-commerce, the Administrative Provisions on protection of children’s online personal information, and the Provisions on mobile Apps personal information collection). This particular formation hints to observers of a field of law that is in continuous development, but this trend can be traced back to the 1990s.

⁴ Five systems constitute the Cybersecurity Law: (1) Cybersecurity Multi-Level Protection Scheme – specific security measures need to be met according to the level of the activities that would affect the public, scaled from 1 the least risky to 5 the most risky; (2) Critical Information Infrastructure Security Protection System (Chapter 3); (3) Personal Information and Important Data Protection System (Chapter 4), which focuses on the scope of personal information protection and the according protection standard; (4) Network Products and Services Management – network products that are used in critical information infrastructure (see number 3) are required to go through a cybersecurity assessment; and (5) Cybersecurity Incident Management System – guidelines and measures are provided to be activated in response to cybersecurity incidents.

The development of the basic principles of personal information protection has gone through two generations [14], and it is now likely to enter the third one:

- The first generation of personal information protection principles is the OECD Guidelines in 1980 [4] and the Convention 108 issued by the Council of Europe in 1981 [26]. These two documents defined the basic regime for a “personal information protection law” in a modern sense.
- The representative legislation of the second generation of personal information protection principles is the EU Data Protection Directive 1995 [23]. It is expanded based on the first-generation principle, adding elements such as “data minimisation”, “deletion”, “sensitive data”, and “independent personal data protection authority” among others.
- The third generation of personal information protection principles is still dominated by the European Union - the GDPR. Compared with the second generation, the GDPR has expanded, including “establishing a data protection officer within the enterprise”, “data protection impact assessment”, “reporting to data protection authorities after data security incidents and notifying individuals”, “collective litigation system” and so on.

In addition to the EU-led progressing, the OECD released a new version of the privacy framework in 2013 without significant changes, mainly introducing the concept of data security breach notice to authority as well as to an individual being affected [4].

Against this background, we switched focus to the nine principles contained in the Asia-Pacific Economic Cooperation Privacy Framework [2]. The principles embodied by APEC are still aligned with the standard of the first generation. While we appreciate the EU’s efforts in promoting the protection of personal information by “willing to do it alone”, other countries seem to be satisfied that the first generation is sufficient. But empirical research shows that countries and regions outside the EU have achieved the personal data protection standard of the second generation by rectifying new/updated personal information protection laws [13]. It is not surprising to see that China’s CSL followed the principles of the APEC privacy framework (see Appendix 1)⁵ while the supplementary norms and state standards⁶ are following the GDPR (see Appendix 2). In order to include a reasonable scope of a comprehensive comparison for meaningful and practical discussion, we refer to China’s personal data protection rules as to the requirements addressed in the CSL and its supplementary norms and standards.

⁵ All the appendices can be found online: <http://bit.ly/39bGd8I>

⁶ Within China, national standards play an important role in implementing higher-level laws and legislations. They are better understood as a quasi-regulation rather than a technical specification or voluntary frameworks typically presented in Western context. Although they are not legally binding, the competent authorities often refer to them when conducting assessments and approvals. The bundle of standards under the umbrella of the CSL in practice will function as a form of regulation where auditing and certification of the entities will be conducted based on the criteria. Up to date, over 240 national standards related to the field have been issued since 2010.

2.2 Commonalities between the GDPR and the CSL

Even though the GDPR and the CSL are established based on different origins, the convergence between Europe and China’s approaches in personal information protection regime is ever-growing. One of the most glaring similarities between GDPR and China’s data protection laws is the fundamental principles for the processing of personal information (see Appendix 1).

The CSL has also established a bundle of new or more explicit “personal information rights”, including “data correction right”, “right of deletion”, “re-use and breach notification obligation”. However, these principles are drafted in such a high-level that in practice it is unlikely to be directly applied. Instead, the “Information Security Technology - Personal Information Security Specifications” (referred to as “the Specification”), which came into effect in May 2018, turned to be an essential supporting document for the interpretation of Chapter 4 of the CSL. In drafting the Specification, it referenced and benchmarked the current international rules and legislative standards, as well as foreign legislations in the protection of personal information, including the GDPR, OECD Guidelines, APEC Privacy Framework [2], EU-US Privacy Shield agreement, American Consumer Privacy Bill of Rights Act [3].

2.3 Differences between the GDPR and the CSL

Firstly, the CSL provides only ONE legal basis for the processing of personal information – the consent (Art. 41 CSL). The GDPR provides five other legal basis, including the “joker card” – a legitimate interest (Art. 5 GDPR). The requirements for obtaining the consent in the CSL, therefore, is relatively looser than the ones in the GDPR, since it applies to broader scenarios. The GDPR is more indulgent about certain kinds of consent requirements for collecting personal information. Particularly, consent is not strictly required for data sharing under the GDPR [30], Art. 49.

Secondly, “sensitive personal information” under China’s data protection rules is more far-reaching. It is defined as “any personal information that would cause harm to individuals’ reputation, and mental and physical health if illegally disclosed or misused” [28], Art 3(2). Interestingly, ID number, bank account number, credit information and geo-location are included in the category of sensitive personal information, of which the GDPR does not [30], Art. 9.

Thirdly, China’s data protection rules contain more descriptive requirements with regard to security assessment and audit. This is consistent with a broader difference: the objectives of China’s data protection regime overall are to safeguard national cybersecurity. These give it a much broader applicable scope, while GDPR does not.

Last but not least, the major difference between China’s data protection rules and the GDPR is that they have different levels of legal effects. The former is a general description of principles (CSL) with a bundle of recommended standards, while the latter is the EU’s supranational Regulation. Each part of the GDPR is

legally binding, and this legal binding is not only manifested in its specific goal, but also in various ways and measures required to achieve that specific goal.

Additionally, several common elements that exist in other jurisdictions' data protection laws, such as the right to access, right of accuracy and special requirements for sensitive personal data, are still missing in the CSL. The CSL also does not establish a data protection authority at the national level.

3 Operationalization of GDPR and CSL requirements in eHealth IoT scenario

The legal requirements imposed by both the GDPR and the CSL (Appendix 3 and 4) can be divided into two main types: those that influence the processes that stakeholder (healthcare or research institution, hospital, care organization, insurance company, etc.) should execute in the context of a technical solution, and those that influence the design of architectures of IoT applications. The first we call organizational requirements and the second we call technical requirements.

Organizational requirements are the requirements that do not influence the architecture of applications. They are adhered through guidelines, questionnaires, documentation regarding description of processing, justification of the purpose of processing, establishing periodic data audits, informing data subjects on relevant matter, etc. The implementation of organizational requirements can be specific for every use case. Since they are not within the main area of focus, the extended list of these requirements as well as some explanations can be found in Appendix A.

Technical requirements are the requirements that directly influence the architecture of an application. They include establishing data flows for informing the subject, mechanisms for obtaining consent, mechanisms for setting restrictions for processing, authorization, etc. Considering that in contrast to organizational requirements, complying with the technical ones is far from being trivial, in the following subsections we (i) establish a reference eHealth IoT architecture, and (ii) investigate the influence of technical requirements on simplified and reference architectures.

3.1 Reference eHealth IoT architecture

Practical adoption of IoT in the healthcare domain has started several years ago and draw reasonable attention. There were multiple trials for development of eHealth IoT solutions that obtained various levels of success and acceptance. Below we outline a number of related efforts. Habib and Leister [15] proposed an architecture for an eHealth patient monitoring scenario that is based on IoT. It includes the following key elements:

- Sensors (e.g. glucose, body temperature, blood pressure, ECG);
- Smartphone as a hub for sensors;
- Gateway (Wi-Fi or 3G/4G connectivity);

- Stakeholders (e.g. hospital, nursing home, transport, public venues);
- Backend EHR system;
- Health services;
- Corresponding data flows.

Another architecture was presented by Farahani et al. [7]. In that work, the authors introduced a holistic multi-layer IoT eHealth architecture with bidirectional data flows and offered a protocol stack. They split the architecture into three layers: device, fog, and cloud, which reasonably aligns with the ideas in [15].

eHealth IoT solutions rely a lot on wearable devices. This is also supported by Perez and Zeadally in [33]. In their paper that mainly focuses on privacy issues of consumer wearables, the system consists of a personal area network, wearable sensors, smartphones, base stations, cloud storage and analytics. Also, their system highlights a direct communication link between the wearable device and the base station, which is not observed in other publications. The data flows in their work are of both bidirectional and unidirectional types, while the latter observed only between the smartphone and wearables.

In [27], El-Sappagh et al. propose a comprehensive mobile health framework with an integrated clinical decision support system (CDSS) capability. They propose an ontology that is able to collect, formalize, integrate, analyse, and manipulate all types of patient data which provides patients with care plans. Also, the proposed CDSS provides real-time patient monitoring based on vital signs collected from patients' wireless body area networks. The architecture of the proposed framework includes the following elements:

- Wireless body area network (e.g. Bluetooth, Wi-Fi);
- Wireless base unit (e.g. smartphone);
- Wireless router (e.g. Wi-Fi access point);
- Cloud-based environment;
- Backend EHR system;
- Health services;
- Corresponding data flows.

In [21] Fernandez et al. propose a cloud-IoT architecture aiming at protecting the sensitive data of the user by allowing them to control which kind of data is transmitted by their devices and providing supportive tools for agreement visualisation and privacy-utility trade-off. The architecture consists of several layers, from IoT objects in the lower layer to web and mobile applications in the top layer, with regulated communication mechanisms to transfer data from the lower level to data processing services in the top level. The proposed architecture includes user, platform that manages data emanating from IoT devices, cloud repository, service provider, and corresponding data flows. Additionally, the proposed example considers multiple potential stakeholders.

Considering the state-of-the-art discussed above, we establish a reference eHealth IoT architecture (depicted on Figure 1) that consists of:

- Human user - a person which operates the architecture and is a data subject in the solution's context;
- Firmware-driven device - a mobile or embedded device with limited functionality, connectivity scope, and computational resources which operates under commands of a firmware (smart watch/mattress/necklace/plate/glasses/scales/toothbrush/headband/scale, etc.)
- OS-driven device - a mobile device with broad functionality and connectivity scopes that offers advanced memory management (smartphone, smart hub, etc.);
- Gateway - a device or devices that are used for connection with the server's network;
- Controller's server - a device on which data controller stores or processes the data obtained from the user;
- Stakeholder's server - a device on which a stakeholder (governmental health-care institutions, research institutions, hospitals, care organizations, insurance companies, etc.) user data obtained from the data controller.

Fig. 1. Reference eHealth IoT architecture

In this architecture, both the firmware-driven and OS-driven devices are responsible for data collection and represent sensors that can be responsible for providing electroencephalogram (EEG), electrocardiogram (ECG), galvanic skin response (GSR), polysomnogram (PSG), temperature, pressure, humidity, and others.

In its turn, the controller's server, as well as OS-driven device, are expected to perform data-driven services like activity monitoring, sleep monitoring, medication intake monitoring, nutrition analysis, cough detection, fall detection, emotion monitoring, monitoring of physical parameters (heart rate, blood pressure,

weight, etc.), monitoring of environment (air pressure/quality, water quality, humidity, CO2 level, amount of light, noise level, etc.), and other potentially relevant services. In cases like fog computing, gateway may also be involved in performing some computations for the services. However, in this paper we consider it as a purely communicational element which puts the gateway out of the scope of elements that can be manipulated for satisfying the requirements.

The data flows that are also depicted on Figure 1 also influence the architecture and may consist of various data types. To provide a better understanding of relations between the elements of the proposed reference eHealth IoT architecture, we introduce an overview of the data flows in Table 1.

Table 1. Overview of data flows

Origin	Destination	Type of information in the data flow
Human user	OS-driven device	User and sensor input
Human user	Firmware-driven device	User and sensor input
OS-driven device	Human user	Progress notifications, recommendations
Firmware-driven device	Human user	Short version or summary of recommendations, progress notifications
OS-driven device	Firmware-driven device	Software updates, data requests, application commands, progress updates, notifications
Firmware-driven device	OS-driven device	Data collected by sensors, application status updates
OS-driven device	Gateway	Raw or pre-processed sensor input from the devices
Firmware-driven device	Gateway	Data collected by sensors
Gateway	OS-driven device	Software updates for devices, results of analytics, recommendations
Gateway	Firmware-driven device	Notifications
Gateway	Controller's server	Raw or pre-processed sensor input from the devices, data collected by sensors
Controller's server	Gateway	Software updates for devices, results of analytics, recommendations, notifications
Controller's server	Stakeholder's server	Anonymized or pseudonymized data, raw or processed data that are sharable accordingly to the consent
Stakeholder's server	Controller's server	Data that are useful for improving quality of analytics

3.2 Influence of technical requirements on the reference architecture

The main principles behind privacy and data protection by design imply that the technical requirements extracted from the GDPR and the CSL should be taken into consideration from the initial stages of the development of eHealth IoT applications. Therefore, in this subsection we provide (i) an overview of the influence of the GDPR and the CSL requirements on data flows in a simplified architecture, and (ii) an extension of the reference eHealth IoT architecture with identified requirements-driven elements for simultaneous compliance.

Highlighting the influence of technical requirements on architectures is not a trivial task. Therefore, we focus our investigation on analysis of corresponding data flow diagrams (DFDs) that in its turn enable understanding of influence and consequences. This decision is driven by the fact that DFDs are the core elements of STRIDE [20] and LINDDUN [22] methodologies, which are also seen by us as potential drivers of continuous compliance. Additionally, LINDDUN is also used by Ekdahl and Nyman in [10] for an investigation on GDPR compliance, and by Bisztray and Gruschka in [8] for investigation related to Privacy Impact Assessment. Furthermore, Sion et al. in [19], as well as Dewitte et al. in [24], use this methodology for investigations related to Data Protection by Design.

In order to satisfy the technical requirements, we came up with the concepts of services and centres for data flow diagrams. We do not position them as an extension of existing DFD elements (entity, process, data store, data flow, trust boundary), but as aggregators of processes. Subsequently, the services are combinations of several processes that perform certain manipulations on data. In their turn, the centres are combinations of services that need to take place for performing necessary data manipulations.

Based on our findings, we introduce the following additional elements on the DFDs in this section:

- Consent centre – a collection of services responsible for obtaining consent from the user and interpreting it into suitable input for the processing;
- Access/disclosure centre – a collection of services responsible for logging and managing the access to the collected data for given entities under certain conditions (who can get the data);
- Centre of processing permissions/restrictions – a collection of services responsible for establishing lawful processing for involved entities in the context of a given solution (what can be done with the data);
- Data export centre – a collection of services responsible for providing disclosable data in a readable format to a 3rd party or the human user;
- Read/write service – a collection of processes responsible for inserting new data into the database and providing stored data to relevant entities;
- Data correction service – a collection of processes responsible for finding data that needs to be corrected in the database and sending corresponding requests to appropriate services;
- Data deletion service – a collection of processes responsible for finding and deleting certain data in the database;

- Keep data alive service – a collection of processes responsible for timely deletion of irrelevant data from the database;
- Database – an organized collection of data obtained from the data subject;
- Backup – a copy of database taken and stored elsewhere for restoring the original data in case of a data loss event.

Influence of the technical requirements of GDPR. As discussed above, the data flow diagrams are a suitable means for architecture analysis. Therefore, in order to understand the implications of the technical requirements from the GDPR, we extended a simplified reference architecture with relevant centres, services and related data flows (see Figure 2). Furthermore, the usage of DFDs is even strongly justified by the GDPR requirements on accountability documentation.

Fig. 2. Influence of technical requirements from the GDPR on DFDs

As mentioned above, Figure 2 contains a simplified version of the reference eHealth IoT architecture modified accordingly to the technical requirements. In their turn, the relevant requirements can be grouped in the following categories:

1. Initialization (requirements 3, 11);
2. Data management (requirements 7, 8, 9, 13, 15, 16, 17);
3. Security (requirements 7, 9, 18, 19, 22).

The initialization category provides means for informing the user about what data the application will collect, how the application will process the data, and

why such processing is required. Also, it provides information regarding the data controller and data processors, as well as the legal basis and the purpose of processing. The initialization, along with the consent collection, is covered by the consent centre.

The data management category provides support for data storage, data correction and deletion, restriction of processing, logging, data export, and consent withdrawal. Additionally, due to the requirements 8 and 17 that demand logical separation of data entries that enables targeted deletion and usage of structured machine-readable formats, the database is expected to be relational. We recognize that this can be a strong technical constraint, but we leave further investigations on this issue for future work. All the additional elements on Figure 2, except backup and data flows, are responsible for covering this category.

The security category provides support for authorization, data integrity, encryption, data loss prevention, and logging. This category is covered by access/disclosure centre, backup, and the data flows. The latter are expected to run on the protocols that provide data integrity and encrypted communication. Nevertheless, some of the GDPR requirements on security are formulated rather vaguely. For example, requirement 9 and 19 demands applying security best practices and state-of-the-art security measures considering risks and costs. We acknowledge that this was done to accommodate for the reality that best practices, as well as state-of-the-art, changes rapidly with the course of time, and regulations cannot adapt that fast, but this leads to additional efforts for finding reasonable security measures for every particular case and cannot be reflected on the given DFD.

Completeness of the proposed approach can be proven by the fact that the data subjects rights highlighted in the GDPR (the right to information access/accuracy/erasure, right to restrict processing, portability, and right to reject) can be provided by the introduced elements.

Influence of the technical requirements of CSL. In order to understand the implications of the technical requirements imposed by the CSL, we extended a simplified reference architecture with relevant centres, services and related data flows. Considering the smaller amount of requirements that arise from this law than from the GDPR, the influence of the CSL is smaller too, which is depicted on Figure 3. Therefore, some of the elements that can be found on Figure 2 can not be found on Figure 3.

The technical requirements that arise from the Cybersecurity law include:

- Obtaining consent from the subject and informing him/her regarding the purpose, means, and scope of data collection (requirement 1) - covered by consent centre;
- Disclosing collected data only to authorized entities (requirement 2) - covered by access/disclosure centre;
- Preventing data leakages, and data losses (requirement 4) - covered by access/disclosure centre and backup;

Fig. 3. Influence of technical requirements from CSL on DFDs

- Deleting data in case of misuse (requirement 5) - covered by read/write service, data correction service, data deletion service;
- Correcting data in case of necessity (requirement 5) - covered by read/write service, data correction service, data deletion service.

Completeness of the proposed approach can be proven by the fact that the data subjects rights highlighted in the CSL (the right to delete, and the right to rectification) can be provided by the introduced elements.

Simultaneous compliance with the technical requirements of GDPR and CSL. Being compliant with both the GDPR and the CSL is of great interest for eHealth IoT solution providers that operate on European and Chinese markets. We investigated how the architecture of a solution should be adapted to be in line with both legislations. Such adaptation can be reached via extending the reference architecture depicted on Figure 1 with our findings introduced on Figure 2 and Figure 3.

Extending the reference eHealth IoT architecture with the proposed centres and services requires positioning them under the boundaries of devices. Considering that the centres consist of complex processes, they may require partial execution on multiple devices. For example, the formulation of the consent shall take place on the controller's side, while obtaining the actual consent is expected to take place on the OS-driven device's side. Similar issues arise for other centres too. Therefore, access/disclosure, consent, and processing permissions/restrictions centres had to be represented in several instances across the devices that are involved in storing or processing of undisclosable data. Despite

being very similar, their functionality may not be identical and is foreseen to be device- and solution-tailored.

Fig. 4. DFD of a reference eHealth IoT architecture extended with the requirements-driven elements. Grey elements are optional for CSL-only compliance.

Furthermore, Figure 4, on which the extended DFD of the reference architecture is depicted, contains an additional element - functionality of devices. This element represents processes, services, and software that eHealth IoT devices may normally have. They may include heart rate measurements, sleep analytics, notifications, progress reporting, etc.

Additionally, some of the elements on the diagram in question are toned in grey. Inclusion of those elements is obligatory for satisfying GDPR requirements but remain optional for satisfying the CSL.

4 Conclusion and Future Work

This paper presents a comparison of the GDPR and the CSL, and discusses requirements that can be obtained from them on the basis of a case study. Our findings show that simultaneous compliance with both legislations for the eHealth IoT solutions can be reached through (i) obtaining legal requirements from the regulations and laws, (ii) interpreting the legal requirements into technical and organizational ones, (iii) integrating the corresponding services and centres that satisfy technical requirements into solutions architecture.

Considering that our work contributes to the operationalization of the GDPR and the CSL, one of the key findings is that despite some clear differences between these legislations, simultaneous compliance with both of them can be reached in an effective manner. Furthermore, the integration of the proposed elements commits to reducing risks to the fundamental privacy rights of the data subjects in the context of eHealth, and to the reduction of risk that IoT solutions will only be applicable in a single geographical location.

We foresee our future work in this direction to include analysis of applicable standards and relevant sectoral laws, investigation on the requirements for cross-border data transfers, and examination of the practical implications of the usage of relational databases for human input as well as other unstructured content in the GDPR context.

Acknowledgements. This research is funded by Philips Research, Research Fund KU Leuven, and the HEART project (www.heart-itn.eu). This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 766139. This publication reflects only the authors' view and the REA is not responsible for any use that may be made of the information it contains.

References

1. HHealth related Activity Recognition system based on IoT, <http://http://heart-itn.eu/>
2. APEC Privacy Framework, Asia-Pacific Economic Cooperation, Electronic Commerce Steering Group (ECSG) (2005)
3. Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy (2012)
4. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013)
5. Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe (2018)
6. Ayala-Rivera, V., Pasquale, L.: The grace period has ended: An approach to operationalize GDPR requirements. In: Proceedings of 26th International Requirements Engineering Conference (RE). IEEE, Banff, Canada (8 2018)
7. Bahar Farahani, Farshad Firouzi, V.C.M.B.N.C.K.M.: Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems* **78** (2018)
8. Bisztray, T., Gruschka, N.: Privacy impact assessment: Comparing methodologies with a focus on practicality. In: Proceedings of NordSec 2019. p. 3–19 (2019)
9. Brodin, M.: A framework for GDPR compliance for small and medium-sized enterprises. *European Journal for Security Research* p. 243–264 (2019)
10. Ekdahl, A., Nyman, L.: A Methodology to Validate Compliance to the GDPR. Master's thesis, Department of Computer Science and Engineering, Chalmers University of Technology, University of Gothenburg, Gothenburg, Sweden (2018)
11. Erickson, A.: Comparative analysis of the EU's GDPR and Brazil's LGPD: Enforcement challenges with the LGPD. *Brooklyn Journal of International Law* **44** (2019)

12. Fernandes, M., da Silva, A.R., Gonçalves, A.: Specification of personal data protection requirements : Analysis of legal requirements based on the GDPR regulation (2018)
13. Graham Greenleaf, S.L.: China's New Cybersecurity Law – Also a Data Privacy Law? (2016)
14. Greenleaf, G.: Asian Data Privacy Laws. Oxford, United Kingdom (2014)
15. Habib, K., Leister, W.: Threats identification for the smart internet of things in ehealth and adaptive security countermeasures. In: Proceedings of the 7th International Conference on New Technologies, Mobility and Security (NTMS). vol. 555. IEEE, Nashville, Tennessee
16. Han, S.W., Munir, A.B.: Information security technology - personal information security specification: China's version of the GDPR. European Data Protection Law Review (EDPL) **4**, 535–541 (2018)
17. Hintze, M., LaFever, G.: Meeting upcoming GDPR requirements while maximizing the full value of data analytics (2017)
18. Huth, D., Matthes, F.: “appropriate technical and organizational measures”: Identifying privacy engineering approaches to meet GDPR requirements. In: Proceedings of 25th Americas Conference on Information Systems (2019)
19. Laurens Sion, Pierre Dewitte, D.V.L.K.W.I.E.P.V., Joosen, W.: An Architectural View for Data Protection by Design. In: Proceedings of the 2019 IEEE International Conference on Software Architecture (ICSA). IEEE, Hamburg, Germany (2019)
20. Loren Kohnfelder, P.G.: The threats to our products. Microsoft Interface (April 1999)
21. Maribel Fernandez, J.J., Thuraisingham, B.: Privacy-preserving architecture for Cloud-IoT platforms. In: Proceedings of the International Conference on Web Services (ICWS). vol. 555. IEEE (2019)
22. Mina Deng, Kim Wuyts, R.S.B.P.W.J.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering Journal **16**, 3–32 (2011)
23. Parliament, E., Council: 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 (1995)
24. Pierre Dewitte, Kim Wuyts, L.S.D.V.L.I.E.P.V., Joosen, W.: A Comparison of System Description Models for Data Protection by Design. In: SAC 19: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing. p. 1512–1515 (2019)
25. Sandra Dominique Ringmann, H.L., Waldvogel, M.: Requirements for Legally Compliant Software Based on the GDPR. In: Proceedings of OTM 2018: On the Move to Meaningful Internet Systems. pp. 258–276. OTM (2018)
26. Secretary General of the Council of Europe: Convention for the protection of individuals with regard to automatic processing of personal data (1981)
27. Shaker El-Sappagh, Farman Ali, A.H.J.H.J., Kwak, K.S.: A mobile health monitoring-and-treatment system based on integration of the SSN sensor ontology and the HL7 FHIR standard. BMC Medical Informatics and Decision Making **19** (2019)
28. Standing Committee of the People's Congress: Cybersecurity Law (2016)
29. Tovino, S.A.: The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons. Seton Hall law review (2017)
30. Union, E.: Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing

- of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the EU (L 119), 1–88 (May 2016)
31. Voigt, P., von dem Bussche, A.: (2017)
 32. Wang Han, S., M.A.: Practitioner’s Corner Information Security Technology – Personal Information Security Specification: China’s Version of the GDPR? European Data Protection Law Review **4**, 535–541 (April 2018)
 33. Zeadally, S., Perez, A.J.: Privacy issues and solutions for consumer wearables. IT Professional **20** (2018)