Bus Inf Syst Eng
DOI 10.1007/s12599-015-0373-5

RESEARCH PAPER

Legal Compatibility as a Characteristic of Sociotechnical Systems

Goals and Standardized Requirements

**Axel Hoffmann · Thomas Schulz · Julia Zirfas ·
Holger Hoffmann · Alexander Roßnagel ·
Jan Marco Leimeister**

Received: 6 September 2013 / Accepted: 11 June 2014

Abstract Legal compatibility as a characteristic of sociotechnical systems aims at the greatest possible compliance with higher-order legal goals for minimizing social risks of technical systems and extends legality, which refers to the prevention of lawlessness. The paper analyzes the criteria for legal compatibility by reviewing specifications of legally compatible systems and shows goals and resulting requirements to foster legal compatibility. These comprise the following areas: avoiding personal reference in data, ensuring information security, enabling freedom of decision, increasing transparency, ensuring traceability, and increasing usability, whereby traceability and the avoidance of personal reference pursue conflicting goals. The presentation of the goals including their dependencies, relationships, and conflicts in form of standardized requirements explains legal compatibility and summarizes the requirements necessary for the development of legally compatible systems.

Keywords Legal compatibility · Requirements · Requirement patterns

1 Introduction

Legal compatibility as a characteristic of sociotechnical systems is based on legally compatible technology design (Roßnagel 1989). It requires the greatest possible compliance with higher-order legal goals in order to minimize the social risks from the use of technical systems and derives requirements from the fundamental, consistently valid legal norms of the upper levels of the legal hierarchy (Roßnagel 1989). Ideally this would mean, for example, not only to ensure a minimum level of protection of personal data, but also to protect this data in the best way possible. However,

Accepted after one revision by Prof. Dr. Jarke.

Electronic supplementary material The online version of this article (doi:10.1007/s12599-015-0373-5) contains supplementary material, which is available to authorized users.

Dr. A. Hoffmann (✉) · Prof. Dr. J. M. Leimeister
Information Systems, Research Center for Information System Design (ITeG), University of Kassel, Pfannkuchstr. 1,
34121 Kassel, Germany
e-mail: axel.hoffmann@uni-kassel.de

Prof. Dr. J. M. Leimeister
e-mail: leimeister@uni-kassel.de; janmarco.leimeister@unisg.ch

T. Schulz · J. Zirfas · Prof. Dr. A. Roßnagel
Public Law Particularly Environmental Law and Technology Law, Research Center for Information System Design (ITeG), University of Kassel, Pfannkuchstr. 1, 34121 Kassel, Germany
e-mail: t.schulz@uni-kassel.de

J. Zirfas
e-mail: j.zirfas@uni-kassel.de

Prof. Dr. A. Roßnagel
e-mail: a.rossnagel@uni-kassel.de

PD Dr. H. Hoffmann
Competence Center Business Performance, Fraunhofer-Institut für Arbeitswirtschaft und Organisation, Nobelstraße 12,
70569 Stuttgart, Germany
e-mail: holger.hoffmann@iao.fraunhofer.de

Prof. Dr. J. M. Leimeister
Institute of Information Management, University of St. Gallen,
Müller-Friedberg-Str. 8, 9000 St. Gallen, Switzerland

Published online: 03 March 2015

this approach is contrary to the common practice in systems development, which is to identify solutions abiding to statutes and regulations only to the extent to avoid the threat of legal consequences. Among others, the approach of legal compatibility was used for deriving requirements for RFID systems (Müller and Handy 2005), Location Based Services (Jandt 2008), and similar further applications (Bräunlich et al. 2011; Gitter 2007; Hammer et al. 1993; Pordesch and Roßnagel 1994; Ranke 2004; Steidle 2005).

Applications, i.e. software systems supporting users to conduct particular tasks or solve problems, are typically not used in an isolated way but exist within social and organizational environments, making them parts of sociotechnical systems (Berkovich et al. 2014). Legally compatible applications consider the rights and protective needs of the users and therefore are considered to be superior to other applications from a legal perspective. During requirements elicitation, however, it remains largely unclear what specifically is needed for ensuring legal compatibility and what the consequences for sociotechnical system development are. Thus, the explicit consideration of legal compatibility in the development of applications is very rare. One reason is that the use of legal methods, which are applied for deriving such requirements from legal norms, is more or less limited to people with legal expertise or training. For software development teams, with a technical background, this task is difficult to accomplish, resulting in uncertainty concerning the characteristics of a legally acceptable application and concerning the resulting requirements in the technical development process (Hoffmann et al. 2013a). At this point, our proposed requirement patterns come into play. Instead of having to start from scratch and deduct technical requirements from legal texts, requirement analysts can derive technical requirements for their systems based on these templates. By providing pattern catalogs for legally compatible requirement patterns, we relieve them from directly working with legal texts, such as laws, regulations, guidelines, etc.

In order to explain the construct of legal compatibility and to facilitate the practical consideration of relevant requirements, this paper examines documented requirements of legal compatibility for sociotechnical systems and uses these to extract an overview of the most important goals and requirements. These requirements are suitable for reuse in various application development projects. This reduces the need for integrating external experts into the development process while still enabling developers to consider legal compatibility in applications development right from the beginning. This helps to improve the application's quality, reduce development costs, and prevent follow-up costs resulting from disregarded requirements. The research questions we base our work on are:

1. Which requirements increase the legal compatibility of sociotechnical systems?
2. Which are the resulting requirement patterns to be considered for the legal compatibility of sociotechnical systems?

The research questions' objective is to identify which requirements for legal compatibility are used or should be used in the development of sociotechnical systems in order to translate them into reusable requirement patterns. Requirement patterns are an approach for the reuse of requirements (Franch et al. 2010) in that they help analysts to identify and document requirements for new applications (Robertson and Robertson 2006, p. 303 ff.).

In general, a pattern describes a problem which appears frequently and elucidates the essence of the problem's solution (Alexander 1979). Requirement patterns are used for requirements elicitation and analysis. There are various approaches differing in scope, presentation and areas of application (Franch et al. 2010; Henninger and Corrêa 2007). The requirement patterns developed here are based on approaches using patterns to develop specifications (Hoffmann et al. 2014; Renault et al. 2009a, b; Withall 2008). To determine the requirement patterns of legal compatibility, a document analysis is used. The investigated objects are documented requirement collections of technical systems abiding to legal compatibility. The evaluation of the documents is performed by means of a qualitative content analysis (Bortz and Döring 2006; Mayring 2000). Based on the approach of Withall (2008), requirement patterns are created.

In order to structure the requirements of legal compatibility and to provide support to analysts during specification of sociotechnical systems, this paper provides detailed requirement patterns. These include objectives, connections, and dependencies and provide templates with standardized requirements and extensions that can be adopted and adapted for the specification of applications (Hoffmann et al. 2013b).

The paper is organized as follows. First, the fundamentals of legal requirements and legal compatibility are described. Section 3 then deals with the document analysis which was used as research method. Then Sect. 4 describes fields and categories covering the requirements of legal compatibility, before we summarize legally compatible requirements and dwell on dependencies, connections, and conflicts.

2 Legal Compatibility in Technology Design

In order to describe legal compatibility, the next sections show the importance of legal requirements, the challenges which may arise during legal requirements elicitation as well as specific techniques for the elicitation. Following this, the notion of legal compatibility is discussed.

2.1 Importance of Legal Requirements

The legally compliant design of applications is an important challenge in requirements elicitation (Kiyavitskaya et al. 2008; Otto and Anton 2007). For instance, this trend can be observed in the financial services and healthcare industry (Maxwell and Anton 2009), but is also becoming more important in other areas. For ensuring a legally compliant design, the providers must comply with legal regulations aiming at the social balance of interests (Siena et al. 2008). Legal requirements for design result from international and national regulations as well as laws on different levels of the legal hierarchy and various fields of law (Kiyavitskaya et al. 2008). In Germany, in particular the EU Data Protection Directive, the general rights of personality given in article 2 of the constitution with its two manifestations, the right to informational self-determination and the right to confidentiality and integrity of information technology systems, the telecommunications privacy, and on subconstitutional law level the data and consumer protection law have to be considered during applications development (Jandt 2008). Violations of these laws and regulations may result in high costs, e.g., for compensation or penalties (Massey et al. 2009). These costs which may arise from legal actions are increasing faster than all other development costs, and even often exceed the costs of programming (Cosgrove 2001). Only the consideration of legal rules and regulations as well as the application's compliance with these, enables legally compliant systems development (Toval et al. 2002).

The diversity of legal requirements also means that they cannot be fulfilled by just adding individual software components or application features. Their impact typically covers the whole application (Ishikawa et al. 2009). Thus, legal requirements must be considered already during requirements elicitation in order to ensure their fulfillment by means of a legally compliant design at an early stage (Siena et al. 2008). A verdict after legal action on the legality of a technical solution can only allow or disallow the application. Hence, in case of a negative decision law might become an obstacle to technology development (see Roßnagel 2008).

Although the access to statutes and regulations has become easier for analysts in the Internet age (Otto and Anton 2007), the problem of the complexity of applying these cannot be solved. Even the identification of relevant laws and especially the derivation of functional and non-functional requirements from these regulations for the application can hardly be accomplished without legal expertise. Requirements analysts have to be in a position to understand the context and to recognize the contents of the regulations in regard to technical questions despite specific legal formulations and reference modes (Breaux et al. 2006, 2008). Thus, laws and regulations lead to a number of challenges due to numerous ambiguities, cross-references, and specific definitions (Maxwell et al. 2011).

2.2 Elicitation of Legal Requirements

Laws are normative regulations (Penzenstadler and Leuser 2008) which describe what is allowed and what is not allowed. The way in which such laws are formulated differs fundamentally from the way in which requirements are specified (Siena et al. 2008). In determining the legal requirements for an application mainly the following challenges have to be met (Hoffmann et al. 2012; Kiyavitskaya et al. 2008):

- selection of relevant laws
- extraction of relevant obligations and rights from the complex legislation
- abstractness and technological neutrality of the rules
- dynamics of the rules

Since analysts usually have no legal training, legal requirements should be analyzed and introduced to the development process by legal specialists (Kiyavitskaya et al. 2008). However, in requirements elicitation different approaches to treating legal aspects have evolved. A thorough study of legal texts dealing with the requirements elicitation was carried out by Otto and Anton (2007) in order to support analysts in specifying, monitoring, and testing applications in terms of their compliance to legal regulations. This section presents a brief overview of the relevant approaches.

Siena et al. (2008) recommend the transfer of legal requirements into stakeholder goals in order to enable their consideration during goal-oriented requirements elicitation. This approach is also described by Ishikawa et al. (2009). Abstract goals that are set by laws will gradually be refined to technical goals. In order to achieve this, the goals to be reached by a law need to be recognized. The authors point out, however, that the regulations as determined by laws do not correspond to the goals required for requirements elicitation but rather constitute concept definitions which have yet to be made concrete. There is a correlation between the refinement of goals and the refinement of concept definitions (Ishikawa et al. 2009). Also, Guarda and Zannone (2009) deal with legal requirements in a goal-oriented manner. They extract objectives from a law, i.e., the purpose for which the legislation has been passed, and include these during requirements elicitation (Guarda and Zannone 2009). Problems occur when there are no laws or regulations that could be interpreted and thus used directly by the analysts.

Beside this goal-oriented approach there are also papers focusing on the transfer of laws into formal models (Breaux et al. 2008). In that way, it is possible to formally verify if a specification complies with the law. However, the translation of requirements into formal models requires clearly formulated laws, which often is not the case due to the abstractness and technological neutrality of legal norms (Otto and Anton 2007). Even if the regulations provide a sufficient degree of concreteness, the problem of transferring legislative models into requirements still remains (Siena et al. 2008). In addition, methods for the formalization of legislation are still in their infancies and can be used in special cases only (Kiyavitskaya et al. 2008). Thus, it is difficult to use requirements modeling for application development with regard to legal regulations. In addition, abstract laws must be made more concrete in advance.

Toval et al. (2002) prepared a collection of legal requirements in the area of security and privacy of personal data which are meant to support analysts. This collection makes it possible to integrate legal requirements into specifications and thus to develop legally compliant applications. Problems of this approach can be seen mainly in the dynamics of legal regulations and the associated changes to law (Otto and Anton 2007).

2.3 Designing Technology for Legal Compatibility

Dealing with legal requirements in requirement elicitation mainly aims at the applications' compliance with legal regulations (IT Compliance). This prevents an application from violating existing regulations which results in legality. For this purpose, legal regulations are examined for direct or indirect legal requirements which have to be observed during technology design. The Digital Signature Act and the Data Protection Act are prominent examples. From these, direct technical requirements can be obtained which are legally binding since a failure to implement them may have legal consequences. This binding character has led to the understanding of laws and legal regulations as a limiting factor in requirement elicitation. In addition, other laws comprise legal requirements which only indirectly regulate the design of technology, such as § 312e of the German Civil Code (Bürgerliches Gesetzbuch, BGB), imposing legal obligations on an entrepreneur when communicating electronically.

The aim of legal compatibility is to derive technical requirements from the higher-order legal goals which arise from the fundamental, permanently valid legal norms on the upper levels of the legal hierarchy – in particular the constitution (Roßnagel 1993). Legal compatibility (Fig. 1), as the greatest possible compliance with higher-order legal goals in order to minimize the risks of technological systems, goes beyond the concept of legality, which just refers to regulatory compliance as a mandatory requirement (Roßnagel 1989). For example, the requirement of communication privacy arising from the demand for telecommunications secrecy in article 10, paragraph 1 of the Basic Law of the Federal Republic of Germany (Grundgesetz, GG) is implemented in a legally compatible way through automatic communication encryption while waiving this encryption would not be illegal at the same time.

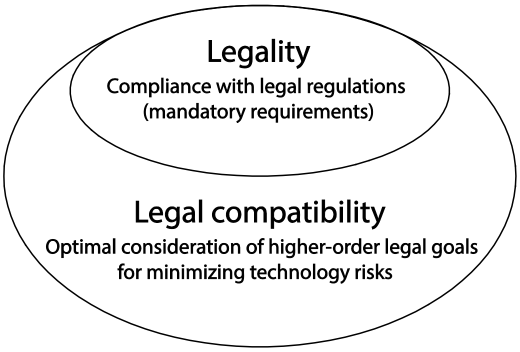
Legality
Compliance with legal regulations
(mandatory requirements)
Legal compatibility
Optimal consideration of higher-order legal goals
for minimizing technology risks

Fig. 1 Legal and legally compatible technology design

Legal compatibility and its reference to permanently valid laws and their objectives as included in the basic laws avoids the necessity to adapt applications as a result of changes to special regulations. In this way requirements can be deduced even when there are gaps in the law as regards detailed regulations. In addition, a legally compatible design may help cover diverse legal situations in different states, without requiring thorough knowledge of detailed regulations. This is a consequence of the fact that the fundamental legal goals of the various states resemble each other more closely than detailed regulations.

3 Extraction of Recurring Requirements Concerning Legal Compatibility

To examine the requirements and their goals resulting from the approach of legally compatible technology design, we use methods of qualitative data collection and evaluation. For data collection, document analysis was used. Documented collections of requirements for technological systems aiming for legal compatibility were the main object of examination.

Starting from the creation of the notion of legal compatibility (Roßnagel 1989, 1993), by means of a forward and backward search eight documents could be identified which deal with requirements of legal compatibility. These were included in the data collection. The documents contain requirements for RFID-based applications (Müller and Handy 2005), location-based services (Jandt 2008), telephone systems (Hammer et al. 1993), electronic signature methods (Pordesch and Roßnagel 1994), mobile commerce applications (Ranke 2004), multimedia assistants (Steidle 2005), software agents (Gitter 2007), and Internet-based elections (Bräunlich et al. 2011). As bases for the requirements, the documents under examination identified the Basic Law of the Federal Republic of Germany (Grundgesetz, GG), the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), the European Data Protection Directive 95/46/EC (Europäische Datenschutzrichtlinie, DSRL), the Code of Civil Procedure (Zivilprozessordnung, ZPO), the Telemedia Act (Telemediengesetz, TMG), the Civil Code (BGB), and the Telecommunications Act (Telekommunikationsgesetz, TKG). The documents were chosen because at least one author of each document is a legal expert, the authors show the same understanding of legal compatibility, and all documents contain a collection of specific requirements concerning legal compatibility. It should be noted that legal compatibility as defined in this paper is applied especially in Germany.

In the following we assume that the requirements of legal compatibility are suited as a source of requirement patterns. Due to their origin in general and permanent legal regulations and due to the objective of the greatest possible compliance with higher-order legal goals, they are suitable for reuse as they ensure persistence of the requirement pattern.

3.1 Data Analysis

The evaluation of the documents was performed using a qualitative content analysis (Bortz and Döring 2006; Mayring 2000). In the first step, the requirements for the applications were extracted from the documents with its derivation of requirements for legal compatibility in order to reduce the quantity of material. In these documents the requirements that were neutral in terms of solutions, as it is intended in requirements elicitation, were called technical design goals. In the documents' table of contents, relevant sections were identified and the design goals were extracted as requirements to be examined. Requirements were reduced to the most important contents. However, we did not adjust them in accordance with the quality criteria for high quality requirements (IEEE 1998) in order to prevent altering the overall meaning of these parts of the text. A total of 152 requirements were extracted from the documents.

In order to ensure understandability of the legal concepts in the requirements, in the next step we consulted the documents' explanations for legal terms and used them for the formulation of requirements.

In a last step, the requirements were structured to identify frequently appearing and theoretically interesting requirement areas that are important for the legal compatibility of applications.

In the process of structuring the requirements, we detected obviously identical requirements from different documents and summarized them with reference to the different sources. Thus, the number of requirements could be reduced and the formation of categories could be facilitated (the number of sources for the requirements was maintained during evaluation). The categories were revised in several iterations and checked by three scientists. Different opinions were discussed and resolved by the following three measures: (1) new assignment of a requirement to another category, (2) creation of a new category and inclusion of the requirement(s), and (3) merging of categories and their requirements. The procedure was completed in consensus with all participants.

During the process, 15 categories were generated. 11 requirements could not be assigned to any category due to their singularity caused by special characteristics of the analyzed applications or their fields of application. They were not taken into account for the evaluation of the general goals of legal compatibility. In a further step, the categories were summarized to areas of application with similar goals. In consensus with all researchers, six areas were identified.

The requirement patterns were compiled based on the approach of Withall (2008, p. 43). In addition, the requirement patterns were reviewed by three lawyers in form of an expert assessment (Petter et al. 2010) and could be improved with their help. In doing so, inaccuracies in the formulations could be corrected and the terminology adapted.

3.2 Limitations

For the analysis of the requirements for legal compatibility, we chose a nonreactive method (document analysis) which makes a data collection repeatable and verifiable. All documents used are freely accessible. To ensure objectivity, all categories and areas were formed by common consensus among the authors involved.

The source documents contain requirements for different applications which allows for a generalization of the results. Here, however, we have to point out that for special areas of applications also specific laws may apply. Thus, the resulting collection of requirement patterns is not entirely complete and the legality of an application cannot be guaranteed by using the requirement patterns alone.

To explain the results from the perspective of systems development, the requirements were not put in an order according to the legal criteria. Instead, we chose an order according to their goals. Consequently, the goals of the requirement patterns and areas reported here do not necessarily coincide with the legal criteria and security goals. Hence, the process of forming categories inductively led to the fact that we only describe goals of the requirements which were included in the requirements collection. For the implementation of legal compatibility it is irrelevant whether a goal addresses several legal criteria or if a legal criterion is described by several goals.

4 Requirement Areas and Requirement Patterns

The requirement patterns of legal compatibility cover six areas. Avoiding personal references in data contains requirements for data collection and administration. Ensuring information security entails requirements for access control and infrastructure security. The realization of the freedom of decision calls for statements of consent and a selective use of system functionalities. An increase in transparency is supposed to make application processes easier to understand for the user. Ensuring traceability demands that the user at any time can understand the processes and circumstances of use in the application. Increasing the usability and thus ensuring an intuitive use of the applications is required by legal compatibility to support transparency and freedom of decision. The following section explains the objectives of the areas and categories based on concise requirements. The corresponding requirement patterns are to be found in the Online Appendix. The frequency of the requirements listed below is an indication that they appeared several times in the documents examined and are therefore suitable for the derivation of requirement patterns. The list does not allow for deducing a ranking on the importance for a particular application.

4.1 Avoiding Personal Reference

35 requirements of legally compatible technology design refer to the use of personal data in applications. The Federal Data Protection Act in Germany (Bundesdatenschutzgesetz, BDSG) in § 3.1 defines personal data as “any information concerning the personal or material circumstances of an identified or identifiable natural person (data subject)” (translated from the original; cf. Gola et al. 2012). For the purpose of legal compatibility, personal data should be avoided in the ideal case or, if necessary, should be deleted as quickly as possible. The application should enable the user to alter personal data. The data should be stored in a decentralized way without reference to individuals.

Ten of the evaluated requirements aim for the avoidance of personal data. Data reduction and data economy mean that the processing of personal data is avoided completely or is minimized wherever possible (Gitter 2007, p. 424; Müller and Handy 2005, p. 1157; Ranke 2004, p. 101 ff.; Steidle 2005, p. 338 ff.). According to § 3, sect. 2 BDSG, automated data processing comprises the collection, processing, and use of personal data. For example, a location-based application should only transmit position data when this is necessary for the particular feature (Jandt 2008, p. 372). The billing of the use of a particular functionality should be possible through flat rates in order to prevent the collection of individual (personal) usage behavior (Jandt 2008, p. 372). In dealing with this type of data, the avoidance of data collections is the ultimate goal and provides the most effective protection (requirement pattern R-S-01). When this requirement is consistently implemented, all other requirement patterns of personal data become obsolete.

In processing personal data, the deletion of these data as quickly as possible is requested by five requirements. Personal data should not be kept available longer than is strictly necessary for running the application (Gitter 2007, p. 410 f.). For instance, localization services should delete previously submitted data when updating the position in order to avoid the creation of movement profiles (Jandt 2008, p. 373). Hence, when data relate to a specific period of time they should be deleted by the application in order not to save obsolete information (Steidle 2005, p. 345). When in doubt about future demands for personal data, deletion is always preferable to storage (requirement pattern R-S-02).

In addition to the requirement of automatic deletion by the application as described in the previous pattern, three requirements also request options for the user to update stored personal data. The users themselves should be able to alter, to correct (Ranke 2004, p. 102), or to delete personal data (Steidle 2005, p. 345) if necessary. This may be executed by the responsible authority or by the person concerned in the application (requirement pattern R-S-03) which would comply to the freedom of choice. If the collection and storage of the data are necessary, the user will be able to correct mistakes.

Eight requirements demand an option for the user to utilize an application anonymously unless the individual reference is relevant for use. According to § 3, sect. 6 BDSG, anonymization is described as “the modification of personal data in such a way that the information concerning the personal or material circumstances can no longer or only with a disproportionate investment of time, cost, and labor be assigned to a certain or identifiable natural person" (translated from the original). Anonymous data are not personal data and therefore they are not covered by the data privacy regulations. If a personal reference needs to be established, then the personal data have to be pseudonymized (Gitter 2007, p. 424 f.; Jandt 2008, p. 371 f.; Ranke 2004, p. 101 ff.; Steidle 2005, p. 339 ff.). Pseudonymization is defined by § 3, sect. 6a BDSG as "replacing the name and other identification characteristics by means of an identifier for the purpose of excluding or substantially impeding the identification of the person concerned" (translated from the original). Location-related data should be referred to, e.g., by pseudonyms in order to exclude a direct personal reference (Steidle 2005, p. 341). In this case, the user should at any time be free to use whatever pseudonym he chooses (Gitter 2007, p. 425 f.; Steidle 2005, p 344). Anonymity is mandatory for elections when any attribution of personal data to individuals cannot be tolerated at all (Bräunlich et al. 2011, p. 134). Anonymization and pseudonymization are expected to prevent or at least to impede the attribution of personal data to a specific user (requirement pattern R-S-04).

For the storage of personal data, ten requirements demand a decentralized storage. Data with personal references should not be kept centrally (Gitter 2007, p. 409 f.; Ranke 2004, p. 104; Steidle 2005, p. 340). Any personal data should be stored separately from data with other contents (requirement pattern R-S-05). For example, data for specific purposes, such as location and usage related data, are to be kept separately (Jandt 2008, p. 371; Müller and Handy 2005, p. 1158; Steidle 2005, p. 341 f.). If possible, the storage of personal data should be on one medium and under the sole disposition of the user (Jandt 2008, p. 371; Ranke 2004, p. 104; Steidle 2005, p. 338). Data control by the user eliminates data protection issues as no regulation exists for the handling of one's own personal data. Abstinence from a central reference file also prevents the combination of data to create a profile and makes it more difficult to draw conclusions about a person.

4.2 Ensuring Information Security

31 requirements of legally compatible technology design refer to the field of information security of applications. In this regard, access to application features and data should be secured. This means that only authorized people should be entitled to gain access to the system. Furthermore, there should also be security mechanisms during communication.

Seven requirements call for data access control mechanisms. Access control means that technical protection measures should be taken to prevent the spying out or manipulation of personal or confidential data (Gitter 2007, p. 411 f.; Jandt 2008, p. 374). Here, three requirements specifically demand an encryption of contents (Gitter 2007, p. 416; Jandt 2008, p. 374; Steidle 2005, p. 345), and thus already define the way of realization during requirement formulation (requirement pattern R-S-06).

In addition to access control for stored data, also unauthorized access to application features should be prevented (Hammer et al. 1993, p. 117). This is demanded by eleven requirements. Compared to the previous requirement pattern, the prevention of access does not refer to the selected access to the data, but to the access via the application (requirement pattern R-S-07). For access control, state-of-the-art protection measures are necessary (Jandt 2008, p. 373).

Besides preventing access for unauthorized people, five requirements claim the possibility to allow third parties selected access (requirement pattern R-S-08). Thus, access control should include the option to grant others access to specific data or features (Hammer et al. 1993, p. 111; Idecke-Lux 2000, p. 240). To achieve this, individual access rights should be assigned either long term (Gitter 2007, p. 413) or for specific situations (Steidle 2005, p. 345). Selected access allows authorized people to perform necessary tasks without requiring the user to grant full access to all application features and data.

Access control for application data should be ensured during communication as well. Eight requirements demand that the transmission of data may not be manipulated (Ranke 2004, p. 274) or spied out (Gitter 2007, p. 413; Jandt 2008, p. 373; Steidle 2005, p. 347) by unauthorized users. A reliable security infrastructure should be used as a basis for realizing this demand (Gitter 2007, p. 429). Along with the access control for data and the avoidance of unauthorized access via the application, a comprehensive security of data can be guaranteed within the system (requirement pattern R-S-09).

4.3 Enabling Freedom of Decision

24 requirements of legally compatible technology design refer to the freedom of decision in the use of particular application features. The user should have agreed to the features and, if needed, should be able to configure the application and waive parts of the application's functionality.

Agreements are demanded by 15 requirements. They aim for the users' consent to all implemented application features (Hammer et al. 1993, p. 97 ff.; Ranke 2004, p. 309). This applies to data collection (Gitter 2007, p. 409; Hammer et al. 1993, p. 109) and data processing through the application (Gitter 2007, p. 418 f.; Jandt 2008, p. 377; Pordesch and Roßnagel 1994, p. 89). For this purpose, the user should be able to decide whether to give an authorization prior to each execution or allow features in general (Gitter 2007, p. 427 f.). In addition, the withdrawal of the user's agreement should be possible. In consenting, the users should be aware of and agree to the consequences of the application's use (requirement pattern R-S-10).

Nine requirements claim configurability, stating that applications should provide multiple usage possibilities to users and keep constraints as low as possible (Steidle 2005, p. 343 f.). The features of an application should be clearly defined and should be usable in a way that they can be switched on and off flexibly. Components of the application should thus be easily removable without the application losing its functionality (Steidle 2005, p. 346 f.). Users should be able to decide which application features they want to use or to block (Gitter 2007, p. 426 f.; Hammer et al. 1993, p. 114). Configurability allows users to give their consent for a specific functionality and, at the same time, allows them to refuse consent to unwanted functionalities of the same application (requirement pattern R-S-11).

4.4 Increasing Transparency

There were 26 requirements of legally compatible technology design which refer to an increase of transparency. An application's functionality and processes should be explained to the user. In addition, the application should show which features are currently executed.

Explanations of processes in applications are demanded by nine requirements. This aims at the transparent presentation of data-processing operations, of data structures, and of the application itself (Müller and Handy 2005, p. 1157; Ranke 2004, p. 301 f.; Steidle 2005, p. 342 f.). Transparency and controllability of data collection and data processing operations are particularly emphasized in the requirements (Steidle 2005, p. 346). However, this aspect also refers to the process of conducting business in which users have to be notified of all essential parts of a contract (Ranke 2004, p. 310). While communicating via an application, the users must also have the possibility to request information to identify their communication partner (Hammer et al. 1993, p. 93). Thus, processes within an application remain transparent for the users (requirement pattern R-S-12).

In addition, 17 requirements demand that an application shows its current functional status (requirement pattern R-S-13) in order to keep the user informed about the state or status of the application (Hammer et al. 1993, p. 95). If the application requires the collection of personal data, for example, by microphones or locations of the users, they should be informed about this feature (Gitter 2007, p. 408; Jandt 2008, p. 374 f.; Ranke 2004, p. 273 f.). In addition, the basic circumstances of a communicative situation should be transparent for the user (Ranke 2004, p. 273; Steidle 2005, p. 342). This helps with the decision whether to control data processing or to cancel it (Hammer et al. 1993, p. 104 f.; Jandt 2008, p. 373; Steidle 2005, p. 344).

4.5 Ensuring Traceability

16 requirements of legally compatible technology design refer to traceability. The application should trace executed processes and a person's identification should always be possible for user statements.

Eight requirements demand a recording of all relevant processes by the application (requirement pattern R-S-14). For traceability of gathering personal data, it is requested to keep logs for subsequent checks (Steidle 2005, p. 346). These should be time-stamped to ensure the suitability of proof (Gitter 2007, p. 422). Furthermore, declarations and confirmations of the user should be stored by the application (Gitter 2007, p. 421 ff.). Compliance with the requirements ensures that the application's behavior may be reconstructed and examined.

In order to improve traceability, eight requirements claim an identification (requirement pattern R-S-15). Signatures should be used as a prerequisite for authenticity and integrity (Jandt 2008, p. 377; Ranke 2004, p. 309 f.; Steidle 2005, p. 339). Thus, declarations by the application's user should be signed for the purpose of assignment and proof suitability (Gitter 2007, p. 417). Ensuring identification improves the validity of the records for subsequent traceability.

4.6 Increasing Usability

Nine requirements of legally compatible technology design demand measures to increase the usability of applications. This involves the operation in general (Jandt 2008, p. 375 f.; Steidle 2005, p. 344) which should be designed in compliance with the user's role. To assist the user, certain elements of the user interface, such as clear marks, are requested (Pordesch and Roßnagel 1994, p. 89). Also, an undo function for user entries should exist (Pordesch and Roßnagel 1994, p. 89). The user should be assisted by means of explanations for certain application steps (Gitter 2007, p. 426 f.; Steidle 2005, p. 346 f.) and proposals for action should be submitted (Pordesch and Roßnagel 1994, p. 89). Since usability is an autonomous field of software quality (ISO 25010 2011, p. 7) it is not considered further here.

5 Discussion

Table 1 presents an overview of the sections and categories as well as the corresponding requirements from the different sources. The numbers indicate how many

Table 1 Number of requirements in each area

Requirement pattern	Müller and Handy (2005)	Jandt (2008)	Hammer et al. (1993)	Pordesch and Roßnagel (1994)	Ranke (2004)	Steidle (2005)	Gitter (2007)	Bräunlich et al. (2011)	Number of requirements in total
Avoiding personal references									
R-S-01: Avoiding personal data	2	3			1	2	2		10
R-S-02: Deleting personal data		1				3	1		5
R-S-03: Modifying personal data					1	2			3
R-S-04: Deleting personal reference		1			1	3	2	1	8
R-S-05: Decentralization of personal data	1	2			2	3	1		9
Total	3	7			5	13	6	1	35
Ensuring information security									
R-S-06: Access control for data		2	1			1	2	1	7
R-S-07: Access control for application features	1	1	4		1	1	2	1	11
R-S-08: Enabling selected access			1			2	2		5
R-S-09: Access control for communication		1			1	2	3	1	8
Total	1	4	6		2	6	9	3	31
Enabling freedom of decision									
R-S-10: Agreement to functionality		1	8	1	2		3		15
R-S-11: Configurability			3			4	2		9
Total		1	11	1	2	4	5		24
Increasing transparency									
R-S-12: Explanation of processes	1		2		2	3		1	9
R-S-13: Displaying application status		3	5		4	2	3		17
Total	1	3	7		6	5	3	1	26
Ensuring traceability									
R-S-14: Recording of processes				2		2	4		8
R-S-15: Ensuring identification		1		3	1	1	2		8
Total		1		5	1	3	6		16
Increasing usability		1		5		2	1		9
Non-assigned requirements	1	1	1	3			2	3	11
Number of requirements in total	6	18	25	14	16	33	32	8	152

requirements were incorporated in the requirement pattern and thus illustrate that the requirements recur and are suitable for requirement patterns.

The requirements from the sources show that usability is a factor of legal compatibility. However, it is not possible derive conclusive requirement patterns due to their diversity. They are most likely linked to the area of transparency since both requirement patterns are aimed at providing the user with a better insight into the application. All factors of legal compatibility which were identified in the previous sections are shown in Fig. 2.

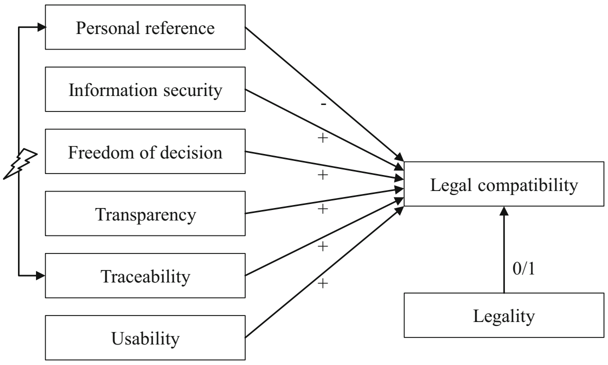

Fig. 2 Areas of legal compatibility

Legal compatibility differs from legality in the way that it cannot be either met or not met, but allows for a comparative assessment of various applications. The categories of the areas where an impact on legal compatibility was recognized are: personal reference, information security, freedom of decision, transparency, traceability, and usability. Personal reference and traceability influence each other mutually. Here, personal reference has a negative impact, traceability as well as the other factors, however, have a positive impact on legal compatibility. An application can only be legally compatible if it fully meets the requirements of legality.

The requirements of legal compatibility are highly interrelated. Requirements with similar objectives were consolidated by being allocated to special focus areas. Hence, the area of avoiding personal references includes the processing of personal data. Applications should collect as little data as possible, and any personal reference, if not absolutely necessary, should be removed. Stored personal data should be deleted as soon as possible if they are not essential for the functionality of the application. Here, the avoidance of personal references is in contrast to the aspect of ensuring traceability. This requirement demands that the user can check data processing activities of the application in retrospect. However, records concerning the processing of personal data are to be treated as personal data and hence must also be minimized. Here, it is necessary to know the opposing goals to enhance legal compatibility and to balance the various interests in the applications' development.

The requirement concerning the decentralization of personal data is associated with the access control for data in the field of information security. The latter requires protective technical measures to entirely prevent access to the data. The requirement for decentralization aims at impeding inappropriate use of personal data and at preventing the combination of data to personal profiles even if access is possible. Hence, this requirement is best implemented by storing personal data solely on a device which is under control of the different users and where data is not collected centrally in personal profiles.

The aspect of transparency comprises requirements that provide user insights into the application. The user should know with whom he is communicating via the application, understand the internal processes, and be informed of active functionality or data processing operations at the time of execution. This area is linked to the area of traceability. Transparency is necessary before and during the use of the application, traceability refers to the possibility of verifying the activities retrospectively.

6 Conclusion

This paper examines the scope and characteristics of requirements concerning legal compatibility. Legal compatibility differs from legality in the way that legal compatibility not only strives for compliance to lawful statutes and regulations, but also takes the compliance with higher-order legal goals into account. The following areas were considered to be of importance for legal compatibility: avoiding personal reference in data, ensuring information security, enabling freedom of decision, increasing transparency, ensuring traceability, and increasing usability. The areas are partially linked with each other. A conflict exists between the avoidance of personal references and ensuring traceability. The results help explain legal compatibility with regard to applications on a theoretical basis. The requirement patterns with their goals, dependencies, connections, and conflicts presented in this paper make it possible to consider legal compatibility from the beginning of the development process in the specifications of applications for socio-technical systems.

The requirement patterns can be taken as a basis for considering legal compatibility in development projects. However, so far the focus is on the fundamentals of the data protection law. Legal compatibility, on the other hand, does not restrict the legal area in question. Hence, requirement patterns in other areas, such as administrative law and enterprise compliance policies, seem possible as well. Future research should also examine the actual use of the requirement patterns. The requirement patterns should be applied in different companies in order to have them tested by experienced and less experienced requirement analysts, which may help identifying their added value for development projects.

References

Alexander C (1979) The timeless way of building. Oxford University Press, New York

Berkovich M, Leimeister J, Hoffmann A, Krcmar H (2014) A requirements data model for product service systems. Requir Eng 19(2):161–186. doi:10.1007/s00766-012-0164-1

Bortz J, Döring N (2006) Forschungsmethoden und evaluation, 4th edn. Springer, Heidelberg

Bräunlich K, Richter P, Grimm R, Roßnagel A (2011) Verbindung von CC-Schutzprofilen mit der Methode rechtlicher IT-Gestaltung KORA – Anwendungsbeispiel: Wahlgeheimnis. Datenschutz und Datensicherheit (DuD) 35(2):129–135

Breaux TD, Vail MW, Anton AI (2006) Towards regulatory compliance: extracting rights and obligations to align requirements with regulations. In: 14th IEEE international requirements engineering conference, pp 49–58

Breaux TD, Anton AI, Boucher K, Dorfman M (2008) Legal requirements, compliance and practice: an industry case study in accessibility. In: 16th IEEE international requirements engineering conference, pp 43–52

Cosgrove J (2001) Software engineering and the law. IEEE Softw 18(3):14–16

Franch X, Palomares C, Quer C, Renault S, De Lazzer F (2010) a metamodel for software requirement patterns. In: 16th international working conference on requirements engineering: foundation for software quality (REFSQ), Essen, Germany, pp 85–90

Gitter R (2007) Softwareagenten im elektronischen Geschäftsverkehr – Rechtliche Vorgaben und Gestaltungsvorschläge. Nomos, Baden-Baden

Gola P, Klug C, Körffer B, Schomerus R (2012) BDSG Bundesdatenschutzgesetz – Kommentar, 11th edn. Beck, München

Guarda P, Zannone N (2009) Towards the development of privacy-aware systems. Inf Softw Technol 51(2):337–350

Hammer V, Pordesch U, Roßnagel A (1993) Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet. Springer, Heidelberg

Henninger S, Corrêa V (2007) Software pattern communities: current practices and challenges. In: CSE Technical Reports, ACM, paper 52

Hoffmann A, Schulz T, Hoffmann H, Jandt S, Roßnagel A, Leimeister JM (2012) Towards the use of software requirement patterns for legal requirements. In: Seyff N, Madhavji NH (eds) 2nd international requirements engineering efficiency workshop (REEW 2012) at REFSQ 2012. ICB, Essen, Germany, pp 50–61

Hoffmann A, Bittner EAC, Leimeister JM (2013a) The emergence of mutual and shared understanding in the system development process. In: Doerr J, Opdahl AL (eds) 19th international working conference on requirements engineering: foundation for software quality (REFSQ). Springer, Essen, Germany, pp 174–189

Hoffmann A, Hoffmann H, Söllner M (2013b) Fostering initial trust in applications – developing and evaluating requirement patterns for application websites. In: 21th European conference on information systems (ECIS), Utrecht, Netherlands

Hoffmann A, Söllner M, Hoffmann H, Leimeister JM (2014) Requirement patterns to support socio-technical system design. In: David K, Geihs K, Leimeister JM, Roßnagel A, Schmidt L, Stumme G, Wacker A (eds) Socio-technical design of ubiquitous computing systems. Springer, Heidelberg, pp 191–209

Idecke-Lux S (2000) Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz. Nomos, Baden-Baden

IEEE (1998) IEEE recommended practice for software requirements specifications. IEEE, New York

Ishikawa F, Inoue R, Honiden S (2009) Modeling, analyzing and weaving legal interpretations in goal-oriented requirements engineering. In: Proceedings of the 2nd international workshop on requirements engineering and law, pp 39–44

ISO 25010 (2011) Systems and software engineering – systems and software quality requirements and evaluation (SQuaRE) – systems and software quality models. International Organization for Standardization (ISO), Geneva

Jandt S (2008) Vertrauen im Mobile Commerce – Vorschläge für die rechtsverträgliche Gestaltung von Location Based Services. Nomos, Baden-Baden

Kiyavitskaya N, Krausova A, Zannone N (2008) Why eliciting and managing legal requirements is hard. In: Proceedings of requirements engineering and law, pp 26–30

Massey AK, Otto PN, Anton AI (2009) Prioritizing legal requirements. In: Proceedings of the 2nd international workshop on requirements engineering and law, pp 27–32

Maxwell JC, Anton AI (2009) Developing production rule models to aid in acquiring requirements from legal texts. In: 17th IEEE international requirements engineering conference, pp 101–110

Maxwell JC, Antón AI, Swire P (2011) A legal cross-references taxonomy for identifying conflicting software requirements. In: 19th IEEE international requirement engineering conference, pp 197–206

Mayring P (2000) Qualitative content analysis. Forum Qualitative Sozialforschung (Forum Qual Soc Res) 1(2)

Müller J, Handy M (2005) RFID als Technik des Ubiquitous Computing – Eine Gefahr für die Privatsphäre? In: Ferstl OK, Sinz EJ, Eckert S, Isselhorst T (eds) Wirtschaftsinformatik 2005. Physica, Heidelberg, pp 1145–1164

Otto PN, Anton AI (2007) Addressing legal requirements in requirements engineering. In: 15th IEEE international requirements engineering conference, pp 5–14

Penzenstadler B, Leuser J (2008) Complying with law for RE in the automotive domain. In: Proceedings of requirements engineering and law, pp 11–15

Petter S, Khazanchi D, Murphy JD (2010) A design science based evaluation framework for patterns. SIGMIS Database 41(3):9–26. doi:10.1145/1851175.1851177

Pordesch U, Roßnagel A (1994) Elektronische Signaturverfahren rechtsgemäß gestaltet. DuD 2(94):82–91

Ranke JS (2004) M-Commerce und seine rechtsadäquate Gestaltung – Vorschläge für vertrauenswürdige mobile Kommunikationsnetze und -dienste. Nomos, Baden-Baden

Renault S, Mendez-Bonilla O, Franch X, Quer C (2009a) PABRE: pattern-based requirements elicitation. In: Proceedings of the third international conference on research challenges in information science (RCIS), pp 81–92

Renault S, Mendez-Bonilla O, Franch X, Quer C (2009b) A pattern-based method for building requirements documents in call-for-tender processes. Int J Comput Sci Appl 6(5):175–202

Robertson S, Robertson J (2006) Mastering the requirements process. Addison-Wesley Professional, Boston

Roßnagel A (1989) Freiheit im Griff: Informationsgesellschaft und Grundgesetz. Hirzel, Stuttgart

Roßnagel A (1993) Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin. Nomos, Baden-Baden

Roßnagel A (2008) Rechtswissenschaftliche Gestaltung der Informationstechnik. In: Von Kortzfleisch HF, Bohl O (eds) Wissen, Vernetzung, Virtualisierung. Eul, Köln

Siena A, Mylopoulos J, Perini A, Susi A (2008) From laws to requirements. In: Proceedings of requirements engineering and law, pp 6–10

Steidle R (2005) Multimedia-Assistenten im Betrieb – Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme. DUV, Wiesbaden

Toval A, Olmos A, Piattini M (2002) Legal requirements reuse: a critical success factor for requirements quality and personal data protection. In: 10th IEEE international requirements engineering conference, pp 95–103

Withall S (2008) Software requirement patterns. Microsoft Press, Redmond