Accepted Manuscript online: 2022-09-23 Article published online: 2022-12-15

3LGM2IHE: Requirements for Data-Protection-Compliant Research Infrastructures—A Systematic Comparison of Theory and Practice-Oriented Implementation

Robert Gött[1] Sebastian Stäubert[2] Alexander Strübing[2] Alfred Winter[2] Angela Merzweiler[3] Björn Bergh[4] Knut Kaulke[5] Thomas Bahls[1] Wolfgang Hoffmann[1] Martin Bialke[1]

[1] Department Epidemiology of Health Care and Community Health, Institute for Community Medicine, University Medicine Greifswald, Greifswald, Germany
[2] Institute of Medical Informatics, Statistics and Epidemiology (IMISE), Leipzig University, Leipzig, Germany
[3] Institute for Medical Informatics, Heidelberg University Hospital, Heidelberg, Germany
[4] Institute for Medical Informatics and Statistics, Kiel University, University Hospital Schleswig-Holstein, Kiel, Germany
[5] Technology, Methods and Infrastructure for Networked Medical Research, Berlin, Germany

Address for correspondence Robert Gött, Dipl.-Ing., Department Epidemiology of Health Care and Community Health, Institute for Community Medicine, University Medicine Greifswald, Ellernholzstr. 1-2, 17487 Greifswald, Germany (e-mail: robert.goett@uni-greifswald.de).

Methods Inf Med 2022;61:e134–e148.

Abstract

Objectives The TMF (Technology, Methods, and Infrastructure for Networked Medical Research) Data Protection Guide (TMF-DP) makes path-breaking recommendations on the subject of data protection in research projects. It includes comprehensive requirements for applications such as patient lists, pseudonymization services, and consent management services. Nevertheless, it lacks a structured, categorized list of requirements for simplified application in research projects and systematic evaluation. The 3LGM2IHE ("Three-layer Graphbased meta model - Integrating the Healthcare Enterprise [IHE]") project is funded by the German Research Foundation (DFG). 3LGM2IHE aims to define modeling paradigms and implement modeling tools for planning health care information systems. In addition, one of the goals is to create and publish 3LGM^2 information system architecture design patterns (short "design patterns") for the community as design models in terms of a framework. A structured list of data protection-related requirements based on the TMF-DP is a precondition to integrate functions (3LGM^2 Domain Layer) and building blocks (3LGM^2 Logical Tool Layer) in 3LGM^2 design patterns.

Methods In order to structure the continuous text of the TMF-DP, requirement types were defined in a first step. In a second step, dependencies and delineations of the definitions were identified. In a third step, the requirements from the TMF-DP were systematically extracted. Based on the identified lists of requirements, a fourth step

Keywords
- informed consents
- General Data Protection Regulation
- record linkage
- consent management
- pseudonymization

received
February 16, 2022
accepted after revision
September 23, 2022
accepted manuscript online
September 23, 2022
article published online
December 9, 2022

DOI https://doi.org/10.1055/a-1950-2791.
ISSN 0026-1270.

Georg Thieme Verlag KG, Rüdigerstraße 14, 70469 Stuttgart, Germany

included the comparison of the identified requirements with exemplary open source tools as provided by the "Independent Trusted Third Party of the University Medicine Greifswald" (TTP tools).

Results As a result, four lists of requirements were created, which contain requirements for the "patient list", the "pseudonymization service", and the "consent management", as well as cross-component requirements from the TMF-DP chapter 6 in a structured form. Further to requirements (1), possible variants (2) of implementations (to fulfill a single requirement) and recommendations (3) were identified. A comparison of the requirements lists with the functional scopes of the open source tools E-PIX (record linkage), gPAS (pseudonym management), and gICS (consent management) has shown that these fulfill more than 80% of the requirements.

Conclusions A structured set of data protection-related requirements facilitates a systematic evaluation of implementations with respect to the fulfillment of the TMF-DP guidelines. These re-usable lists provide a decision aid for the selection of suitable tools for new research projects. As a result, these lists form the basis for the development of data protection-related 3LGM^2 design patterns as part of the 3LGM2IHE project.

Introduction

The TMF Data Protection Guide Supports Medical Research in Germany

The TMF (Technology, Methods, and Infrastructure for Networked Medical Research) "Guidelines for Data Protection in Medical Research Projects" (TMF-DP)[1] deal with the data protection-compliant implementation of medical research projects. The guidelines are acknowledged by the state data protection authorities. Both technical and organizational measures can be derived from the recommendations in the guide. These measures can be supported by variants of software implementations (so-called application systems), e.g. for generating pseudonyms or patient/proband identifiers (PIDs) and for managing consent documents. These application systems can be combined into 3LGM^2 design patterns, which can be used to create concrete information technology (IT) security concepts for a research project. In particular chapter 6 of the TMF-DP is the subject of further consideration, as it contains requirements for the application systems of a Trusted Third Party (TTP). Nevertheless, it lacks a structured, categorized list of requirements for simplified application in research projects and systematic evaluation.

The 3LGM2IHE Project Supports the Planning of Interoperable IT Architectures

3LGM2IHE (Three-Layer Graph-based Meta Model—Integrating the Healthcare Enterprise) is a Deutsche Forschungsgemeinschaft (DFG)-funded collaborative project (Grant Number BI 1930/2–2, 2019–2022) of the University of Leipzig (Prof. Alfred Winter), Heidelberg University Hospital (Angela Merzweiler), Kiel University (Prof. Bergh), University Medicine Greifswald (UMG; Martin Bialke) and TMF.

In this context 3LGM^2 represents a modeling paradigm and tool for the planning of information systems in health care, which has been used in teaching and in medical informatics projects for many years.

In the first funding phase (2016–2018) of the 3LGM2IHE project, an approach for modeling information systems via the 3LGM^2 toolbox and IHE (Integrating the Healthcare Enterprise) was developed.

This concept will now be expanded in the second funding phase (2019–2022) to include suitable design patterns and common IT architectures. The aim is to take into account current technical developments and the requirements of the community (usability, user experience, user acceptance) to significantly simplify the planning of interoperable and low-error IT architectures for medical research projects, also with regard to the topic of data protection.

3LGM^2 design patterns for data protection demand a 3LGM^2 Domain Layer (in terms of functions or structured requirements) and 3LGM^2 Logical Tool Layer (in terms of building blocks or software functionalities).

Open Source Tools Help Build Privacy-Compliant Research Infrastructures

In order to fulfill data protection requirements, modular, practical solutions for the application areas of identity management, pseudonymization, and consent management have been developed, published,[2] and made available to the scientific community free of charge under an open source license (AGPL v3) within the DFG-funded MOSAIC project (Grant Number HO 1937/2–1, 2012–2015) (www.ths-greifswald.de). The resulting tools for identity management and record linkage,[3] administration of pseudonyms (gPAS),[2] and consent management (gICS)[4] are used in numerous projects and in a variety of institutions (National Cohort, German Center for Cardiovascular Research e.V., Medical Faculty of RWTH Aachen,[5] Clinical Cancer Registry MV [Mecklenburg, Western Pomerania], DKMS [German Bone Marrow Donor File], Charité

and DFPN [German Research Practice Network], NUM [Network University Medicine]) for the realization of TTP functionalities.[2]

A structured comparison of these TTP tools with the data protection requirements of the TMF-DP has not yet been carried out and forms an essential basis for the development of 3LGM^2 data protection design patterns. Furthermore, such a comparison could also be helpful as a basis for decision-making for future users and the development of research infrastructures.

Objectives

The goal of the work is to identify and systematize the requirements from the TMF-DP in terms of record linkage, pseudonymization, and consent management. The resulting structured lists of requirements allow a comparison with existing tools. The TMF-DP considers the requirements on a methodological level. It is now interesting to present the coverage of requirements by tools that have emerged in practice and through project experience. Are there discrepancies between requirement-driven software development and the requirements of the TMF-DP concept? Such a comparison was made using the tools of the "Independent Trusted Third Party of the University Medicine Greifswald" (TTP). A purpose of this comparison was to check the coverage of the TMF-DP by the provided function of the TTP tools.

Methods

For structuring the contents of a continuous text, the focus and some definitions concerning the delineations of the extraction have to be defined first.

- What is the goal of the structuring process regarding focus or topic?
- Which facts are to be classified or categorized?
- To which essential facts can the structuring be reduced?
- How can the reader be enabled to easily understand the extracted contents?

The application of these definitions leads to a thematically focused extract, which should be easier and faster to grasp than the original full text. At the same time, this method leads to a loss of information concerning other subject areas that are not in the focus of the current consideration.

In the presented case, the use of a tabular representation is sufficient, as the focus is on extracting enumerable requirements and classifying them into requirement types. The requirements are then assigned to the basic components "ID Management"—consisting of the "Patient List" and the "Pseudonymization Service"—and "Consent Management."

Step 1: Categorization of Requirements

First of all, the various requirement types were considered in more detail and classified uniformly. This standardization allows distinguishing one textual content from the other in order to achieve the desired systematic structure.

►Table 1 documents all requirement types that could be derived from the TMF-DP.

The systematic structuring of the requirements took into account the requirement types: "solution variant"—hereafter referred to as "variant"—"recommendation," and functional "requirements."

Organizational requirements that only involve human-to-human interaction were not taken into account, since they do not specify any requirements for a machine or software implementation. Of course, devices can also be involved in a human-to-human interaction, such as "Person A informs person B," but person A needs a working telephone for this interaction. In this case, there would actually be a technical requirement, which, however, is outside the functional scope under consideration and does not have to be listed as a condition, because it is a matter of course. Incidentally, the mapping of human-to-human interactions with the 3LGM^2 tools is quite possible, but rather rarely a modeling goal. Organizational requirements that concern human-to-machine interactions contain requirements for machines or software implementations. These can be described under the requirement type functional requirement.

Methodical requirements do not contain a purely technical description, but describe a method of procedure in general. This category has the character of a guideline and does not result in a technical requirement. Therefore, it is not considered in this publication either.

In the case of functional requirements, a distinction has to be made between the set of requirements that arise as part of an implementation and those that arise from a project. An implementation usually covers requirements from several projects. Requirements arising from a project represent only a subset of the expected requirements of an implementation. A distinction has to therefore to be made between the view of the project and that of the implemented product. In addition, the perspective also influences the prioritization of requirements. The TMF-DP describes, among other things, requirements for TTP implementations that have emerged from a set of well-known projects. This perspective can be interpreted as a specification of product requirements and will be used in the course of the project to compare them with established solutions of the community.

Step 2: Identification of Relationships, Dependencies, and Boundaries

As the terms "function" and "use case" relate to requirements, their meaning and limits have to be specified (►Table 2).

Both terms are not part of the requirement types. However, a function or several related functions can be rephrased as a requirement. The terms "requirement," "recommendation," and "solution variant" can be used again as subcategorizations. The "use case" is closely tied to the intended use scenario or project. In a project, use cases are defined in order to check the suitability of a software product and to be able to identify necessary enhancements. The use case is composed of several requirements and is therefore not considered separately in the requirements tables.

Table 1 Classification of requirement types

Term	Subcategory	Description	Example(s)
Requirement	Nonfunctional and organizational	• Tasks that are performed by real persons or groups of persons (areas of responsibility) • What is the procedure in/for this case/event? • Keyword: Standard Operating Procedure (SOP), action steps, human-to-human interactions, or human-to-machine interactions	(1) "Depseudonymization can only be initiated by an authorized institution or by authorized persons according to the rules and regulations of the research association and can only be performed by identity management." (TMF-DP, Ch. 6.1.3.5, p. 117 par. 3) (2) A private key has been compromised. Processing operations that use this key must be stopped immediately. The security vulnerability must be identified and fixed offline. A new private key must be generated and installed. Processing processes can be restarted.
	Nonfunctional and methodical	• No technical description of the requirement, but process-less consideration (may well be part of processes) • Has a factual character	(1) "During this process, suitable mechanisms must be in place to prevent the patient's pseudonym (PSN) used in the research module from being disclosed to unauthorized persons" (TMF-DP, Ch. 5.3.2.6, p. 91 par. 4) (2) A private key must be stored securely from unauthorized persons.
	Functional (technical)	• Digital data are processed • Result data are generated • Keyword: input–output, input–process–output (IPO) model	(1) "The manner in which the patient list operates is intended to ensure that once a patient has been registered, he or she will be recognized again on subsequent reporting." (TMF-DP, Ch. 6.1.1.1 p. 109 par. 0) (2) In the transformation step, the medical data (MDAT) must first be encrypted with the private key and transferred to service XY.
Recommendation		• … it is not obligatory or technically necessary to proceed in this way. • but possibly "Best Practice," generally usual or approved • are to be distinguished from requirements • they represent a possible suggestion how to proceed • Note: As this is an evaluation category, "recommendations" have been included.	"A central user and role directory (e.g., Active Directory) can provide good services for rights and role management, …" (TMF-DP, Ch. 6.2.1.2, p. 131, par. 5)
Variant		• Occasionally a project requirement can be covered by several solution paths • An implementation only needs to support one variant • Solution variants of a topic are to be understood like a requirement (vs. recommendation)	Example from TMF-DP (Ch. 6.1.2, p. 113 par. 3 pt. k)): Variant A—pseudonym assignment list: "In the case of an assignment list that assigns arbitrary pseudonyms … only the case of compromising some or all pseudonyms is relevant. In this case, these must simply be replaced by newly assigned ones …" Variant B—cryptographic pseudonyms: "If the pseudonyms were assigned by a cryptographic transformation, the previous algorithm must be replaced by a new one of sufficient strength; all previously assigned pseudonyms must be replaced by those generated according to the new algorithm."

Table 2 Dependent definitions

Term	Description	Example
Function	A function serves to partially fulfill a functional requirement and a functional requirement might need several different functions (M-to-N relationship). It represents an atomic procedure that is usually used several times. It is not the internal algorithmic description that specifies a function in this context, but primarily its defined behavior.	"The IDAT must be used to verify in the … database whether the patient has already been registered and a PID assigned. If this is not the case, a new PID must be generated and transferred to the patient list dataset with the IDAT." (TMF-DP, Ch. 6.1.1.1 p. 109 par. 0)
Use case	Use cases arise in the context of a project requirement. They have the character of workflows and describe a necessary procedural flow for a specific situation that has to be processed.	"Existing databases are searched for currently contactable subjects with suitable data on the basis of defined inclusion and exclusion criteria. The result is a suggestion list, on the basis of which the subjects are contacted directly by the attending physician or, if consent has been obtained, also from the research project." (TMF-DP, Ch. 3.2.4.5, p. 30, par. 1)

[Use Case] $m \rightarrow n$ [Functional Requirements] $m \rightarrow n$ [Functions].

The following example illustrates two different use cases requiring the same partial function.

1. *Use case—additional pseudonymization step ("second pseudonymization") during data export by a transfer unit (use-and-access procedure)*: by generating application-related "secondary pseudonyms" (PSN2), an accumulation of research data across different research projects is prevented. A "separation of powers" within the transfer unit is not required as part of this pseudonymization step. A transfer unit may have knowledge of the relationship between PSN1 and PSN2.
2. *Use case—pseudonymization of data from health care for data transfer to research repository:* within this pseudonymization step, a "separation of powers" through MDAT (medical data), PSN1, and PID is mandatory.

In both use cases, the "pseudonymization" sub-function works identically. Generic functions would in turn have to support pseudonymization both with (2) and without (1) separation of powers—depending on the use case. These functions may in turn be interpreted as requirements.

Step 3: Systematic Extraction of Requirements from the TMF-DP

Taking into account the definitions and relationships made in steps 1 and 2, the textually described requirements from chapter 6 of the TMF-DP were transformed into a structured, categorized form. The requirements were assigned to the following services.

- Patient list (Record Linkage, short: RL) (►**Table 3**).
- Pseudonymization service (PSN) (►**Table 4**).
- Consent Management (CM) (►**Table 5**).
- Cross-Component (WF) (►**Table 6**).

In addition to the systematic extraction of the requirements, the text analysis also documented relevant facts for further work in the 3LGM2IHE project with regard to the creation of design patterns for data protection tools (like E-PIX, gPAS, gICS) and their interaction based on the TMF data protection concepts. In addition, this resulted in review comments with regard to a new edition of the TMF-DP.

Step 4: Exemplary Matching of the Requirements with the TTP Tools

The lists of requirements generated in step 3 were preassessed in an initial assessment by the first author. This was followed by a separate interview with two product managers from the TTP of the UMG. During the interview, the exact content of each requirement was discussed in detail and, if necessary, the wording of the TMF-DP was consulted again. If no specific software configuration was necessary for the evaluation of the degree of fulfillment, the functions were evaluated using the "Live-Demos of the Trusted Third Party tools E-PIX, gICS, and gPAS."[6]

The consultation identified required support categories that provide information on the degree or type of support provided by the software tools for the respective requirement. Important findings and details were recorded in the requirements tables (►**Tables 3**–**6**) (column "Comment"). The documentation was again done separately for the services "patient list," "pseudonymization service," and "consent management."

The matching was made according to the component–product relationships. "ID Management" splits into a patient list (compared with E-PIX for RL) and a pseudonymization service (compared with gPAS for PSN). The component "Consent Management" (CM) is compared with the consent management service gICS.

Results

(1) Systematized Requirements of the TMF-DP

The TMF-DP combines the components "patient list" and "pseudonymization service" into the term "ID Management"

(chapter 6.1[1]). Requirements mentioned in connection with "ID Management" were then assigned to both services. An example of this is the management of users and their roles and rights. It is necessary in both components, but should be considered per component (compare ►Table 3 [RL–21] and ►Table 4 [PSN–25]).

The column "Ref" indicates the respective requirement. The column "Description" briefly specifies the actual requirement. The column "TMF-DP" contains one or more reference(s) to the TMF-DP. The meaning of the column "Requirement Type" is described in ►Table 1.

►Table 3 shows the list of requirements for a patient list or record linkage that are derived from the TMF-DP. ►Table 4 contains the list of requirements referred to a pseudonymization service. ►Table 5 emerged for consent management. Some requirements identified require higher level processing services. These specific requirements are documented in the fourth requirements list (►Table 6).

Table 3 Requirements according to TMF-DP for the patient list (Record Linkage, short: RL)

Ref	Description	TMF-DP	Requirement type
RL-1	Accept externally generated PID in case of patient/proband registration (IDAT contains PID)	Ch. 6.1.1.1 p. 108 par. 1 pt. 1 Ch. 6.1.1.1 p. 110 par. 3	Requirement
RL-2	In case of patient/proband registration, PID is generated by itself (IDAT does not contain PID)	Ch. 6.1.1.1 p. 108 par. 1 pt. 2	Requirement
RL-3	Additional information (context) on the origin of an identifier or pseudonym, such as reporting office, reporting date, contact person	Ch. 6.1.1.1 p. 108 par. 1 Ch. 6.5.2.4 p. 161 par. 5	Requirement
RL-4	Merge synonymous patient/proband identities using scoring algorithm	Ch. 6.1.1.1 p. 109 par. 0	Requirement
RL-5	Methods for avoiding synonym errors	Ch. 6.1.1.1 p. 109 par. 1	Requirement
RL-6	Methods for avoiding homonym errors	Ch. 6.1.1.1 p. 109 par. 1	Requirement
RL-7	IDAT for inventory reconciliation freely configurable	Ch. 6.1.1.1 p. 109 par. 3	Requirement
RL-8	Inventory reconciliation via error-tolerant algorithm with adjustable sensitivity	Ch. 6.1.1.1 p. 109 par. 4	Requirement
RL-9	Manual merging of synonymous patient/proband identities	Ch. 6.1.1.1 p. 109 par. 5 Ch. 6.1.1.1 p. 110 par. 2	Requirement
RL-10	Registration of a patient/proband takes place (at least) with the reporting location and the time (is stored)	Ch. 6.1.1.1 p. 109 par. 6	Requirement
RL-11	When a patient/proband is recognized, the reporting location and time are overwritten (no history)	Ch. 6.1.1.1 p. 109 par. 6 Ch. 6.5.2.4 p. 162 par. 0	Requirement
RL-12	Anonymization by deleting the entry in the patient/proband list (anonymization process)	Ch. 6.1.2 p. 112 par. 5 Ch. 6.1.2 p. 113 par. 1 (pt. j) Ch. 6.1.3.8 p. 119 par. 2 Ch. 6.1.2 p. 159 par. 1 pt. 2	Requirement
RL-13	Storage of initial and external identifiers in patient/proband list	Ch. 6.1.3.1 p. 114 par. 3	Requirement
RL-14	Storage of pseudonyms in identity management	Ch. 6.1.3.1 p. 114 par. 3	Requirement
RL-15	Initial identifier (PID) in human-readable form	Ch. 6.1.3.1 p. 115 par. 2	Recommendation
RL-16	User front end for patient/proband registration	Ch. 6.1.4.1 p. 119 par. 3	Requirement
RL-17	Front end for handling nonautomatically matched patient/proband identities	Ch. 6.1.4.1 p. 120 par. 0 pt. 2	Requirement
RL-18	Correction of patient/proband data via batch process	Ch. 6.1.4.1 p. 120 par. 0 pt. 3	Requirement
RL-19	User access possible when resolving from PID to IDAT	Ch. 6.1.4.1 p. 120 par. 1	Requirement
RL-20	AD/LDAP connection	Ch. 6.2.1.2 p. 131 par. 5 Ch. 6.2.5.1 p. 136 par. 4	Recommendation
RL-21	Support of different role profiles per user: username + password + role. (see also TMF-DP ch. 6.2.3.3 "Possible role conflicts")	Ch. 6.2.1.3 p. 131 par. 6 Ch. 6.2.3.3 p. 135 par. 1	Requirement
RL-22	Decentralized storage of rights	Ch. 6.2.1.3 p. 132 par. 1 pt. 1	Variant
RL-23	Central storage of rights	Ch. 6.2.1.3 p. 132 par. 1 pt. 2	Variant
RL-24	Knowledge about the access right of physician to patient/proband	Ch. 6.2.1.3 p. 132 par. 2 Ch. 6.5.2.4 p. 161 par. 4	Requirement

(*Continued*)

Table 3 (*Continued*)

Ref	Description	TMF-DP	Requirement type
RL-25	SAML = Security Assertion Markup Language, XACML = eXtensible Access Control Markup Language	Ch. 6.2.5.4 p. 138 par. 1	Recommendation
RL-26	Storage of initial identifiers in patient/proband list—can accept/persist SIC	Ch. 6.4.2.1 p. 146 par. 1	Requirement
RL-27	Storage of initial identifiers in patient/proband list—can generate/persist SIC	Ch. 6.4.2.1 p. 146 par. 1	Requirement
RL-28	ADAT can be stored to the IDAT of the patient/proband	Ch. 6.5.2.4 p. 161 par. 4	Requirement
RL-29	Reference to ADAT can be saved	Ch. 6.5.2.4 p. 161 par. 4	Requirement
RL-30	Support of monitoring and plausibility checks	Ch. 6.8.2.3 p. 187 par. 3	Requirement
RL-31	Support of data reconciliation with external sources (e.g., registration offices, health offices, and registry offices)	Ch. 6.8.3.3 p. 190 par. 3	Requirement
RL-32	Monitoring of synonyms for the revision of record linkage parameters	Ch. 6.8.4 p. 191 par. 3	Requirement
RL-33	Transfer of corrections contained in the patient/proband list to other systems	Ch. 6.8.5 p. 191 par. 4	Requirement

Table 4 Requirements according to TMF-DP for the pseudonymization service (PSN)

Ref	Description	TMF-DP	Requirement type
PSN-1	Visibility of PID/PSN per context (e.g., clinical module, study module, study) and/or user (authorization results from multiple keys, such as user and context).	Ch. 6.1 p. 106 par. 3	Requirement
PSN-2	Management of temporary pseudonyms	Ch. 6.1.1.1 p. 107 par. 1	Requirement
PSN-3	Additional information (context) on the origin of an identifier or pseudonym, such as reporting office, reporting date, contact person (contact)	Ch. 6.1.1.1 p. 108 par. 1 Ch. 6.4.2.1 p. 146 par. 1	Requirement
PSN-4	Create pseudonym for patient/proband based on ID (PSN service)	Ch. 6.1.1.2 p. 110 par. 3	Requirement
PSN-5	Check services involved in the allocation and transport of PSNs	Ch. 6.1.1.2 p. 110 par. 4	Requirement
PSN-6	Pseudonymization service passes encrypted data	Ch. 6.1.1.2 p. 111 par. 1 Ch. 6.4.5 p. 155 par. 4	Requirement
PSN-7	Pseudonymization service conveys data (with temporary keys)	Ch. 6.1.1.2 p. 111 par. 2 Ch. 6.4.5 p. 155 par. 4	Requirement
PSN-8	Creation of a PSN from PID, PSN, or any string (“pseudonymize everything”)	Ch. 6.1.1.2 p. 111 par. 3 Ch. 6.1.2 p. 114 par. 1	Requirement
PSN-9	Depseudonymization of pseudonyms (depseudonymization process)	Ch. 6.1.1.2 p. 111 par. 3 Ch. 6.1.3.2 p. 115 par. 3	Requirement
PSN-10	Notification via interface to order replacement of pseudonyms by unique anonymous keys	Ch. 6.1.2 p. 113 par. 0	Requirement
PSN-11	Exchange of pseudonyms (“re-pseudonymization”)	Ch. 6.1.2 p. 113 par. 2 (pt. k) Ch. 6.4.2.10 p. 152 par. 2	Requirement
PSN-12	Method for ID06.2: case of PSN assignment list	Ch. 6.1.2 p. 113 par. 2 (pt. k) Ch. 6.1.3.6 p. 117 par. 4	Variant
PSN-13	Method for ID06.2: case of cryptographic pseudonym	Ch. 6.1.2 p. 113 par. 3 Ch. 6.1.3.6 p. 118 par. 1	Variant
PSN-14	Notification or interface for the replacement of pseudonyms	Ch. 6.1.2 p. 113 par. 2	Requirement
PSN-15	Create anonymous identifier	Ch. 6.1.2 p. 114 par. 1	Requirement
PSN-16	No data storage in the pseudonymization service (cryptographic pseudonym generation)	Ch. 6.1.3.2 p. 115 par. 3	Recommendation
PSN-17	Pseudonymization interface	Ch. 6.1.3.2 p. 115 par. 3	Requirement

Table 4 (*Continued*)

PSN-18	Secure storage of the transfer algorithm to pseudonyms	Ch. 6.1.3.2 p. 115 par. 4	Requirement
PSN-19	Temporary blocking of pseudonyms (temporary pseudonyms)	Ch. 6.1.3.6 p. 118 par. 2 und 3	Requirement
PSN-20	Creation of pseudonyms from pseudonyms	Ch. 6.1.3.6 p. 118 par. 4	Requirement
PSN-21	Creation of multiple derived pseudonyms (pseudonym hierarchies)	Ch. 6.1.3.6 p. 118 par. 4	Requirement
PSN-22	Re-pseudonymization via symmetric encryption	Ch. 6.1.3.6 p. 118 par. 5	Recommendation
PSN-23	User intervention possible in case of depseudonymization	Ch. 6.1.4.2 p. 120 par. 4	Requirement
PSN-24	AD/LDAP connection	Ch. 6.2.1.2 p. 131 par. 5 Ch. 6.2.5.1 p. 136 par. 4	Recommendation
PSN-25	Support of different role profiles per user: username + password + role. (see also TMF-DP chap. 6.2.3.3 “possible role conflicts”)	Ch. 6.2.1.3 p. 131 par. 6 Ch. 6.2.3.3 p. 135 par. 1	Requirement
PSN-26	Decentralized storage of rights	Ch. 6.2.1.3 p. 132 par. 1 pt. 1	Variant
PSN-27	Central storage of rights	Ch. 6.2.1.3 p. 132 par. 1 pt. 2	Variant
PSN-28	SAML = Security Assertion Markup Language, XACML = extensible Access Control Markup Language	Ch. 6.2.5.4 p. 138 par. 1	Recommendation

Table 5 Requirements according to TMF-DP for Consent Management (CM)

Ref	Description	TMF-DP	Requirement type
CM-1	Notification to delete data	Ch. 6.1.2 p. 112 par. 5 or pt. h, i) Ch. 6.4.2.11 p. 153 par. 5	Requirement
CM-2	Withdrawal possible per consent module (partial withdrawal)	Ch. 6.3.2.8 p. 143 par. 3	Requirement
CM-3	Complete withdrawal possible	Ch. 6.5.2.2 p. 159 par. 1 pt. 1	Requirement
CM-4	Consent can be requested via interface	Ch. 6.6.6 p. 170 par. 3	Requirement
CM-5	Consent module-based and accessible	Ch. 6.6.6 p. 170 par. 5	Requirement
CM-6	Detailed and graduated representation of consent	Ch. 6.6.6 p. 170 par. 5	Requirement
CM-7	Central consent management, coupled with ID management	Ch. 6.6.6 p. 171 par. 1	Requirement
CM-8	Communication of changes in consent	Ch. 6.6.6 p. 171 par. 2	Requirement
CM-9	Support of monitoring and plausibility checks (derived)	Ch. 6.8.2.3 p. 187 par. 3	Requirement

Table 6 Cross-component workflow requirements (WF) according to TMF-DP

Ref	Description	TMF-DP	Requirement type
WF-1	Management of multiple PID/PSN (“identifiers”) per context (e.g., clinical module, study module, study) (optional participation of the pseudonymization service)	Ch. 6.1.1 p. 106 par. 1 Ch. 6.1.1.1 p. 108 par. 4	Requirement
WF-2	Register patient/proband (optional participation of the pseudonymization service)	Ch. 6.1.1.1 p. 107 par. 3	Requirement
WF-3	PID/PSN is derived by cryptographic transformation (not a requirement, but a technical variant)	Ch. 6.1.1.1 p. 108 par. 1	Recommendation
WF-4	Study module triggers MDAT transfer to clinical module (optional patient list participation)	Ch. 6.3.2.1 p. 140 par. 5 pt. b	Requirement
WF-5	Transmission of correction information back to the data source per depseudonymization	Ch. 6.4.2.4 p. 148 par. 3	Requirement

(2) Exemplary Comparison of the Identified Requirements with Solutions Established in the Community

The structured lists of requirements from (1) were exemplarily compared with the functional scope of the open source tools E-PIX (record linkage), gPAS (pseudonym management), and gICS (consent management). The question is to what extent these project-driven components fulfill the conceptually developed requirements catalogue of the TMF-DP.

The consultation of TTP employees and developers resulted in the required support level needed for the evaluation of the degree of fulfillment. The relationship in ►Table 7 resulted from the comparison of the functions of E-PIX and the requirements for a patient list (►Table 3). ►Table 8 shows the results of the comparison of the functions of gPAS and the requirements for a pseudonymization service (►Table 4). The assessments in ►Table 9 resulted from the comparison of the requirements for consent management and functions of the gICS tool (►Table 5). This is followed by an evaluation of the functions (►Table 10) that require cross-component service processing (►Table 6).

The coverage of TMF-DP requirements by the individual components is shown in ►Table 11. The requirement type "Recommendations" is not listed here, as these are optional requirements. Related "variants" have been considered as one requirement and counted as such.

Table 7 Comparison of the functions of E-PIX with the requirements of the TMF-DP (Yes = "The requirement is completely covered by the component"; Yes, alternatively solved = "The requirement is not covered exclusively by the component)

Ref	Yes, supported	Yes, alternatively solved	No, design decision	No, not planned	Requirement type	Comment
RL-1	x				A	Externally generated PIDs can be taken from several source systems
RL-2	x				A	
RL-3	x				A	E-PIX supports identifier and data source domain to document the context of groups of identifiers (description field).
RL-4	x				A	Extensible combinations of distance (e.g., Levenshtein distance) or hash algorithm (e.g., Bloom filter, PPRL) and configurable weighting (e.g., Fellegi–Sunter algorithm) of IDAT components
RL-5	x				A	Extensible combinations of distance (e.g., Levenshtein distance) or hash algorithm (e.g., Bloom filter, PPRL) and configurable weighting (e.g., Fellegi–Sunter algorithm) of IDAT components
RL-6	x				A	Extensible combinations of distance (e.g., Levenshtein distance) or hash algorithm (e.g., Bloom filter, PPRL) and configurable weighting (e.g., Fellegi–Sunter algorithm) of IDAT components
RL-7	x				A	IDAT mandatory fields are freely configurable
RL-8	x				A	Extensible combinations of distance (e.g., Levenshtein distance) or hash algorithm (e.g., Bloom filter, PPRL) and configurable weighting (e.g., Fellegi–Sunter algorithm) of IDAT components
RL-9	x				A	Possible via intuitive web interface and interface (duplicate resolution)

Table 7 (*Continued*)

Ref	Yes, supported	Yes, alternatively solved	No, design decision	No, not planned	Requirement type	Comment
RL-10	x				A	Per registration, the data source and an optional external date can be specified
RL-11				x	A	The history of changes is fully documented in E-PIX, except when deleting IDAT for anonymization purposes
RL-12	x				A	Persons or identities can be deactivated or deleted (including deletion of history).
RL-13	x				A	
RL-14	x				A	
RL-15	x				B	The internal identifier (MPI) can be replaced by formatable pseudonym before publishing (with the help of gPAS)
RL-16	x				A	
RL-17	x				A	
RL-18	x				A	
RL-19				x	A	Manual confirmation of the resolution of a PID in IDAT is not a use case to date
RL-20	x				B	Keycloak connectivity possible
RL-21	x				A	The internal user administration supports the login per role
RL-22	x				C	
RL-23	x				C	Possible through the Keycloak connectivity
RL-24				x	A	No use case from projects to date
RL-25				x	B	No use case from projects to date
RL-26	x				A	
RL-27		x			A	E-PIX can store identifiers or pseudonyms (SICs), but does not generate them itself, this is done by gPAS (pseudonymization service)
RL-28				x	A	No use case from projects to date
RL-29	x				A	A reference can be additionally stored as an externally generated identifier
RL-30	x				A	
RL-31	x				A	
RL-32	x				A	
RL-33		x			A	Only possible in combination with further tool “TTP-Dispatcher“

Note: Additional TTP components are required: No, design decision = “The requirement—as described—is not covered by the component. The developers of the TTP components decided on a different solution concept.” No, not planned = “The requirement is not supported. An implementation is not planned on the part of the developers.” “Requirement type” notation: A = “Requirement”; B = “Recommendation”; C = “Variant.”

Table 8 Comparison of the functions of gPAS with the requirements of the TMF-DP (Yes = "The requirement is completely covered by the component"; Yes, alternatively solved = "The requirement is not covered exclusively by the component)

Ref	Yes, supported	Yes, alternatively solved	No, design decision	No, not planned	Requirement type	Comment
PSN-1		x			A	This would require further IT security measures (separate TTP instances)
PSN-2	x				A	Configuration via the pseudonymization domain
PSN-3	x				A	gPAS supports hierarchical domains to document the context of groups of pseudonyms (description field).
PSN-4	x				A	
PSN-5		x			A	Only possible in combination with further tool "TTP-Dispatcher"
PSN-6			x		A	TTP does not pass through user data (design decision)
PSN-7		x			A	Only possible in combination with further tool "TTP-Dispatcher"
PSN-8	x				A	
PSN-9	x				A	
PSN-10		x			A	Only possible in combination with further tool "TTP-Dispatcher"
PSN-11			x		A	No cryptographic methods are used
PSN-12	x				C	
PSN-13			x		C	The variant of pseudonym assignment is preferred
PSN-14		x			A	Only possible in combination with further tool "TTP-Dispatcher"
PSN-15	x				A	
PSN-16			x		B	The favored variant of pseudonym assignment cannot support this recommendation due to its principle
PSN-17	x				A	
PSN-18			x		A	The favored variant of pseudonym assignment cannot support this requirement due to its principle
PSN-19				x	A	No use case from projects to date
PSN-20	x				A	
PSN-21	x				A	
PSN-22			x		B	The favored variant of pseudonym assignment cannot support this recommendation due to its principle
PSN-23				x	A	The manual confirmation of a depseudonymization request is not a use case so far; for an automated depseudonymization, the authenticity of the requesting system can be checked
PSN-24	x				B	Keycloak connectivity possible
PSN-25	x				A	The internal user administration supports the login per role
PSN-26	x				C	
PSN-27	x				C	Possible through the Keycloak connectivity
PSN-28				x	B	No use case from projects to date

Note: Additional TTP components are required: No, design decision = "The requirement—as described—is not covered by the component. The developers of the TTP components decided on a different solution concept." No, not planned = "The requirement is not supported. An implementation is not planned on the part of the developers." "Requirement type" notation: A = "Requirement"; B = "Recommendation"; C = "Variant."

Table 9 Comparison of the functions of gICS with the requirements of the TMF-DP (Yes = "The requirement is completely covered by the component"; Yes, alternatively solved = "The requirement is not covered exclusively by the component)

Ref	Yes, supported	Yes, alternatively solved	No, design decision	No, not planned	Requirement type	Comment
CM-1		x			A	Only possible in combination with further tool "TTP-Dispatcher"
CM-2	x				A	
CM-3	x				A	
CM-4	x				A	Via REST-FHIR and SOAP
CM-5	x				A	
CM-6	x				A	
CM-7	x				A	
CM-8		x			A	Only possible in combination with further tool "TTP-Dispatcher"
CM-9	x				A	

Note: Additional TTP components are required: No, design decision = "The requirement—as described—is not covered by the component. The developers of the TTP components decided on a different solution concept." No, not planned = "The requirement is not supported. An implementation is not planned on the part of the developers." "Requirement type" notation: A = "Requirement"; B = "Recommendation"; C = "Variant."

Table 10 Comparison of the cross-component processes of TTP tools (TTP-Dispatcher) with the requirements of the TMF-DP (Yes = "The requirement is completely covered by the component"; Yes, alternatively solved = "The requirement is not covered exclusively by the component)

Ref	Yes, supported	Yes, alternatively solved	No, design decision	No, not planned	Requirement type	Comment
WF-1	x				A	
WF-2	x				A	
WF-3			x		B	The variant of the pseudonym assignment is preferred
WF-4	x				A	In combination with further tool "TTP-Dispatcher"
WF-5	x				A	In combination with further tool "TTP-Dispatcher"

Note: Additional TTP components are required: No, design decision = "The requirement—as described—is not covered by the component. The developers of the TTP components decided on a different solution concept." No, not planned = "The requirement is not supported. An implementation is not planned on the part of the developers." "Requirement type" notation: A = "Requirement"; B = "Recommendation"; C = "Variant."

Table 11 Overview of requirements coverage (recommendations omitted)

			E-PIX (RL)		gPAS (PSN)		gICS (CM)		Cross-component (WF)		Sum	
			►Table 7		►Table 8		►Table 9		►Table 10			
			N[a]	%	*N*[a]	%	*N*[a]	%	*N*[a]	%	N[a]	%
		Sum	**28 + 1**	**100%**	**20 + 2**	**100%**	**9**	**100%**	**4**	**100%**	**62 + 3**	**100%**
Support category	Yes	Yes	22 + 1	86.2%	10 + 2	77.2%	7	100%	4	100%	**43 + 3**	**86.2%**
	Yes, alternatively solved		2		5		2		–		**10**	
	No, design decision	No	–	13.8%	3	22.8%	–	–	–	–	**3**	**13.8%**
	No, not planned		4		2		–		–		**6**	

[a]Number of *requirements* [+ Number of requirements from *variants*].

Discussion

►Table 11 shows an 86.2% coverage of the requirements from the TMF-DP by the TTP tools. ►Table 12 lists the unsupported requirements, which account for the remaining 13.8%.

These unfulfilled requirements can be divided into two reasons for nonsupport.

- There has been no such use case from a project so far (affects five requirements).
- Technical or methodical constraints (affects three requirements).

Only one requirement is not supported due to a divergent view of the product owners (RL−11).

The assessment of coverage was purely quantitative. Better than an unweighted quantitative assessment would be a qualitative assessment, i.e., a consideration of the different importance of the individual requirements. This might make it easier to assess the degree of fulfillment and to make a prioritization of requirements.

A qualitative assessment was not the subject of the study and should be considered in a more in-depth analysis in a separate project. This would require a survey of all existing projects that use TTP components. This survey should be conducted individually for each project using a standardized questionnaire and include a prioritization along the lines of "must have" and "nice to have." This information may then be used to derive a generalized weighting based on experience. In the case of projects at an early stage, in which no TTP-relevant software installations exist yet, one could possibly consult already existing data protection concepts of the project to answer the questionnaire.

It was not always possible to find a comprehensive 1:1 correspondence to the software components for all requirements from the TMF-DP. In such cases, a collaborative consideration based on knowledge and experience was made by the product owners together with the first author. The mentioned components offer functions that go beyond the TMF-DP. The TMF-DP specifies requirements depending on the project circumstances and situation, but does not set any limits on the scope of implementation. In regular operation, further requirements have become relevant, such as support for pseudonym hierarchies, multi-identities, modular consent, and withdrawal management as well as federated record linkage. Such requirements arose after 2014 (publication date of the TMF-DP), for example, by supporting federated implementations between decentralized (site) installations and the central data sharing platform in the Medical Informatics Initiative (MII).[7]

Another example of this is the clearer separation of the term "Identity Management" into "Record Linkage" (TMF-DP:

Table 12 Summary of nonsupported requirements

Ref	Description	No, design decision	No, not planned	Comment	Reason
RL-11	When a patient/proband is recognized, the reporting location and time are overwritten (no history)		x	The history of changes is fully documented in E-PIX, except when deleting IDAT for anonymization purposes	–
RL-19	User access possible when resolving from PID to IDAT		x	manual confirmation of the resolution of a PID in IDAT is not a use case to date	1
RL-24	Knowledge about the access right of physician to patient/proband		x	No use case from projects to date	1
RL-28	ADAT can be stored to the IDAT of the patient/proband		x	No use case from projects to date	1
PSN-6	Pseudonymization service passes encrypted data	x		TTP does not pass through user data (design decision)	2
PSN-11	Exchange of pseudonyms ("re-pseudonymization")	x		No cryptographic methods are used	2
PSN-18	Secure storage of the transfer algorithm to pseudonyms	x		The favored variant of pseudonym assignment cannot support this requirement due to its principle	2
PSN-19	Temporary blocking of pseudonyms (temporary pseudonyms)		x	No use case from projects to date	1
PSN-23	User intervention possible in case of depseudonymization		x	The manual confirmation of a depseudonymization request is not a use case so far; for an automated depseudonymization, the authenticity of the requesting system can be checked	1

Abbreviations: IDAT, identifying data; PID, patient/proband identifier.
Note: Reason: 1. There has been no such use case from a project so far (affects five requirements). 2. Due to technical constraints or principles, this requirement cannot be supported in this way (affects three requirements.

Patient list) and "Pseudonymization Management" (TMF-DP: Pseudonymization Service). The first mentions of this distinction can already be found in the TMF-DP (chapter 6.1). This clearer separation is helpful for a more modularized and generic implementation and for the allocation of personnel and technical areas of responsibility. A separation between the components "Record Linkage," "Pseudonymization Management," and "Consent Management" has proven useful in recent years[2] and should be adopted in the revision of the TMF-DP.

When considering the requirements from the TMF-DP on consent management, it is noticeable that the requirements are likely to be incomplete according to current knowledge. After the time of publication (2014), the relevance of managing informed consents increased due to legal developments like the EU General Data Protection Regulation (EU GDPR) and practical reasons. In particular, within the DZHK (German Centre for Cardiovascular Research),[8] requirements for consent management comprise requirements beyond the TMF-DP, amongst others:

- Support in automatically determining the current consent status of a patient.
- Support with quality checks of consents.
- Individualization of modular consent templates.
- Automatic support for consideration of validity dates and validity periods of consent.

Moreover, paperless digital consent management has become much more important since 2014. With regard to a revision of the TMF-DP, it would also make sense to add guidelines that cover recent developments of legal conditions and current project requirements.

It is also becoming apparent that requirements can no longer be covered by a single component (►Table 10), but that a cross-component service is needed to coordinate the complex workflows. In such a component, project-specific processes and the necessary communication paths can be configured or, if necessary, implemented.[2] This reduces the need for project-specific adaptations of the basic components and their project-specific communication with each other.

Conclusions

We extracted a list from the TMF Data Protection Guide (TMF-DP), a comprehensive reference manual in Germany, where items can be checked off. The list of requirements was applied to assess exemplary software components E-PIX (record linkage), gPAS (pseudonym management), and gICS (consent management), developed in the independent Trusted Third Party in Greifswald (TTP). The assessed software tools meet all basic requirements of the TMF-DP. A few exceptions are documented. However, to further prioritize and weigh the requirements, it is necessary to analyze a sufficiently large number of projects. Requirements that have not yet appeared in the project context can be supported by new or extended functions. The list of requirements is extensive and complex, but more tangible than the continuous text variant of the TMF-DP. This presentation variant is also recommended for a revision of the TMF-DP (planned for 2022) in addition to the continuous text.

The lists of requirements (►Tables 3–6) and the matching lists (►Tables 7–10) support the scientific research community in the design of the data infrastructure and its implementation in research projects.

Users who already use the existing TTP tools feel affirmed in their decision to use suitable tools for a data protection-compliant infrastructure. Interested scientists in new research projects who are looking for software tools are provided with re-usable lists of requirements as well as corresponding software tools (covering these requirements) which can help to comply with the regulations of the EU-GDPR.

The results of the assessment (list of requirements, comparison of the requirements with the exemplary tools) form the basis for follow-up activities within the 3LGM2IHE project. With these results, the preconditions for the development of re-usable data-protection design patterns for 3LGM^2 have been created. These design patters aim to simplify the modeling of data protection-compliant infrastructures and the documentation of requirements according to the TMF-DP.

List of Abbreviations

3LGM2 3LGM^2	Three-layer Graph-based meta model (a synonym for its principle)
3LGM2IHE	Three-layer Graph-based meta model - Integrating the Healthcare Enterprise (IHE) (synonym for the 3LGM2IHE project and its current phase)
AD	Active Directory
ADAT	Physician identifier Data (dt. "Arztdaten")
AGPL	GNU Affero General Public License
CM	Consent Management
DFG	German Research Foundation (Deutsche Forschungsgemeinschaft)
E-PIX	Enterprise Identifier Cross-Referencing
gICS	generic Informed Consent Service
gPAS	generic Pseudonym Administration Service
IDAT	Identifying Data, engl. PII
IHE	Integrating the Healthcare Enterprise
IPO model	Input–Process–Output model
KAS+	Hospital information system with native research support (klinisches Arbeitsplatzsystem)
LDAP	Lightweight Directory Access Protocol
MDAT	Medical Data
MII	Medical Informatics Initiative
MIRACUM	Medical Informatics in Research and Care in University Medicine (MI-I Consortium)
PID	Patient/Proband Identifier
PII	Person Identifying Information
PSN	Pseudonym oder Pseudonymisierungsdienst
RL	Record Linkage
SAML	Security Assertion Markup Language
SOP	Standard Operating Procedure
SW	Software

TMF	Technology, Methods and Infrastructure for Networked Medical Research e.V. (Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.)
TTP	[Independent] Trusted Third Party (TTP) of the University Medicine Greifswald
UMG	University Medicine Greifswald
WF	Workflow
XACML	eXtensible Access Control Markup Language

Statement of Ethical Approval

This research does not require an ethical approval.

Funding

This research was funded by the German Research Foundation (DFG), Grant Number BI 1930/2-2.

Conflict of Interest

None declared.

Acknowledgements

TMF-DP references follow the notation “ch. <chapter> p. <page number> par. <page paragraph> [opt. pt. <bullet point>].” The page paragraph count starts with the first complete paragraph on the respective page. The designation “par. 0” stands for a page-crossing paragraph, which already begins on the preceding page, if the actual quotation is however on the page mentioned. The information refers to the German print edition of the TMF-DP.[1] In tables presented here, the citations originally included have been removed from the TMF-DP. An extended version containing the text quotation is available (upon request to the first author).

References

1 Pommerening K, Drepper J, Helbing K, Ganslandt T. Guideline for Data Protection in Medical Research Projects: TMF's Generic Solutions 2.0. 1st ed. Berlin; MVW; 2014
2 Bialke M, Penndorf P, Wegner T, et al. A workflow-driven approach to integrate generic software modules in a trusted third party. J Transl Med 2015;13:176
3 Hampf C, Geidel L, Zerbe N, et al. Assessment of scalability and performance of the record linkage tool E-PIX® in managing multi-million patients in research projects at a large university hospital in Germany. J Transl Med 2020;18(01):86
4 Rau H, Geidel L, Bialke M, et al. The generic Informed Consent Service gICS®: implementation and benefits of a modular consent software tool to master the challenge of electronic consent management in research. J Transl Med 2020;18(01):287
5 Volmerg J, Bienzeisler J, Klausen A, et al. The technical principles of the ILEG study – preparing the connection of primary and secondary healthcare data, at: https://dx.doi.org/10.3205/21gmds034
6 ths-greifswald.de. Live-demos of the trusted third party tools E-PIX, gICS and gPAS. May 15, 2019. Accessed September 02, 2021, at: https://www.ths-greifswald.de/en/live-demos-of-trusted-third-party-tools/
7 www.medizininformatik-initiative.de. Medical Informatics Initiative – Strengthening research and advancing healthcare. Accessed December 01, 2021, at: https://www.medizininformatik-initiative.de/en
8 Hoffmann W, Rienhoff O. Verfahrensbeschreibung und Datenschutzkonzept des Zentralen Datenmanagements des DZHK. Version 1.2, March 24, 2014, at: https://dzhk.de/fileadmin/user_upload/Datenschutzkonzept_des_DZHK.pdf