EU Data Protection Regulation – Does it Hamper or Support Health System Modernization

Prof. Dr. habil. Bernd Blobel, FACMI, FACHI, FHL7, FEFMI
University of Regensburg, Medical Faculty
PARADIGM CHANGE IN HEALTH SYSTEMS
Paradigm Changes in Health Systems

For improving safety and quality of healthcare as well as efficiency and efficacy of health services processes under the well-known conditions of demographic changes, demanding attitude regarding health and social services, medical and technological progress, development of human resources and the fundamental right for equal care, health systems undergo organizational, methodological and technological paradigm changes.
Paradigm Changes in Health Systems

**Organizational**
- Organization-centric care
- Process-controlled care (DMP)
- Person-centric care

**Methodological**
- General care addressing health problems (one solution fits all)
- Dedicated care (stratification of population for specific clinically relevant conditions)
- Evidence-Based Medicine
- Personalized, preventive, predictive and participative care considering individual health state, conditions and contexts

**Technological**
- Mainframe (KB)
- Client/Server (MB)
- Internet (GB)
- Distributed systems, mobile technologies, nano- and molecular technologies, knowledge representation & management, Kl, Big Data & Business Analytics, Cloud Computing, Social Business (PB, YB)

*Systems Medicine, from art to multi-disciplinary science, from elementary particle to society*
The European Commission put forward its EU Data Protection Reform in January 2012 to make Europe fit for the digital age. More than 90% of Europeans say they want the same data protection rights across the EU – and regardless of where their data is processed.

EU General Data Protection Regulation (GDPR)
http://ec.europa.eu/justice/data-protection/
EU GDPR Content

- Single set of rules and one-stop shop
- Responsibility and accountability
- Consent
- Data Protection Officer
- Pseudonymisation
- Data breaches
- Sanctions
- Right to erasure
- Data portability
- Privacy by Design and by Default
Factors Impacting Data Protection Requirements

**Legal and Regulatory Factors**
- Local or national data protection laws
- International laws
- Work council rules
- Codes of conduct
- Consumer protection legislation

**Contractual Factors**
- Company policies
- Industry regulations
- Professional or technical standards
- Internal control systems
- Third party contracts

**Business Factors**
- Privacy preferences of PII principal
- Normative requirements and guidelines
- Nature of business model or application
- Sensitivity of PII

**Privacy Safeguarding Requirements**
Paradigm Change Consequences for the Assessment of the EU General Data Protection Regulation (GDPR)

• Organizational, methodological and technological paradigm changes in health systems require a multi-disciplinary, international and even global approach from legal, cultural, language, terminology and ontology perspective. This requires the management of multiple domains including multiple policy domains. It is impossible to define processes and policies comprehensively, uniform and legally binding, i.e. in a static way. Complex systems have to be described generically. Their specific sub-systems must be appropriately detailed and interpreted. The aforementioned principles must be applied to the EU General Data Protection Regulation (GDPR) as well.

• Definitions and implementation regulations of the EU GDPR regarding personal data and its processing take account of increasing complexity, variability and dynamics of business cases including healthcare specific ones.
Legal Basics in the Context of Health Systems Development

• Beside the EU GDPR, also the German eHealth law as well as the Law on the protection of critical infrastructures have impacts on health systems.
THE EU GENERAL DATA PROTECTION REGULATION
EU GDPR Definitions

• 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

→Reflection of methodological and technological paradigm changes
EU GDPR Definitions

• 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

→Reflection of methodological and technological paradigm changes when replacing traditional controls
Orientation and Exclusions of the General Data Protection Regulation

- This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons. It intends to harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

- Directive (EU) 2016/680 regulates the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

→Reflection of economic freedom within the Union regarding new business models, also regarding health and welfare systems
EU GDPR Definitions

• 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

→ Necessity of binding explicit policies
Necessity of Explicit, Dynamic Policies 1

- The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

*Necessity of explicit, dynamic policies*
Comprehensive Interoperability by Considering Individual Ontologies

- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Comprehensive interoperability by considering individual ontologies
Comprehensive Interoperability by Considering Individual Ontologies

- The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

→ Comprehensive interoperability by considering individual ontologies
Individual, Dynamic Policies

• Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

→ Individual, dynamic policies
Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

→ Changing the role of the Data Protection Officer towards a risk manager, where risk analysis in dynamic systems must be permanently performed.
• The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

→ Changing the role of the Data Protection Officer towards a risk manager, where risk analysis in dynamic systems must be permanently performed
Explicit and Formally Represented Policies

• **Article 26 Joint controllers:** Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

→ Explicit and formally represented policies
• Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

→ Changing the role of the Data Protection Officer towards a risk manager, where risk analysis in dynamic systems must be permanently performed
Labeling Services

- The data subject’s right of being informed about the processing of personal data as well as rectifying those data if needed can be limited if it proves to be impossible or would involve a disproportionate effort.

→ This problem can be minimized or fully overcome by Labeling
SUMMARY AND CONCLUSIONS
Conclusions 1

- Paradigm changes in health and social care lead to highly distributed, open settings integrating multiple jurisdictional and policy domains, technologies, knowledge and concept representation style, languages, methodologies, interests and attitudes, cultural background and expectations, education and skills, etc., requiring advanced interoperability solutions. The interoperability challenge is not limited to ICT environment, but includes all actors.

- Appropriate security and privacy solutions provide trust and therefore acceptance of health solutions and their IT support.

- Having this crucial role in mind, countries dominating the eHealth and telemedicine scene spend 50% of their budget for security and especially for privacy solutions.

- Security and privacy is not disabling but enabling new technologies.
Conclusions 2

Technologies enabling advanced healthcare setting have to be applied to privacy and security services as well:

- Distributed care paradigm $\Rightarrow$ Distributed security mgnt.
- Mobile health $\Rightarrow$ Mobile security
- Big data and analytics $\Rightarrow$ Big data and analytics for security
- Adaptive systems $\Rightarrow$ Adaptive security and privacy mgnt.
- Person-centered care $\Rightarrow$ Personal policies
- AI $\Rightarrow$ Security intelligence

Build-in Security and Privacy $\Rightarrow$ Security and Privacy by Design

Patient Empowerment
Conclusions 3

• The proposed systems-oriented, architecture-centric, ontology-based and policy-driven approach enables flexible and intelligent interoperability of ubiquitous personalized health services by automatically harmonizing manifold stakeholder groups’ different perspectives and their concept representations.

• The solution has been implemented and demonstrated, e.g. at HIMSS 2013.

In Summary:

• The EU Data Protection Regulation enables arrangements – The paradigm changes in health and welfare systems require arrangements. Realizing this process in an optimal way is a big challenge today and in future. For that purpose, advanced technical-organizational privacy must be implemented and the actors must be trained.
Conclusions 4

- Definition, harmonization, and enforcement of policies must be automated (PIP, PDP, PEP).
- For that reason, policies must be represented comprehensively and formally.
- Security and privacy management will be increasingly model-driven, ontology-based, and automated.
- This doesn’t deliberate us from using privacy-friendly technologies (de-identification by anonymization or pseudonymization resp., encryption, analyzing data collections, etc.)
- Perimeter security and privacy approach must be replaced by a data-driven and data-centric approach.
- Checking compliance with regulations will be replaced by case-specific, individualized and therefore continuous controls and risk management according to the DSM.
Summary

• Existing architecture frameworks just represent ICT-dependent views.
• Also the viewpoints presented are restricted to the ICT process, thereby ignoring the ICT-independent real world business processes relevant for the transformative healthcare eco-system.
• Therefore, existing architecture frameworks are completely based on ICT ontologies such as the HL7 RIM, SOA ontology, etc.
• Contrary to the ISO Interoperability Reference Architecture Model, those architecture frameworks do not follow a consistent abstract system representation.
• They do not consider an architectural composition/decomposition inevitable for managing the complexity of real world systems like the highly complex life-science eco-systems.
• Existing architecture frameworks do not support interdisciplinary approaches to interoperability. Furthermore, most are incompatible.
Summary

• A system-theoretical, architecture centered modeling approach provides the common basis needed.
• Different perspectives on the system are represented by different ontologies to be harmonized for the sake interoperability.
• Ontology design and management as well as knowledge management and representation have to follow the GCM principles and processes.
• The outcome will be intelligent, adaptive systems for advanced eHealth and pHealth.
• The GCM approach enables harmonization between existing specifications. Therefore, it has been selected.
• In transformative healthcare, security, privacy and trust are crucial elements defining the acceptance of any solution.
• Interoperability is first of all not an ICT challenge but a matter of multi-disciplinary cooperation.
Thank you very much for your kind attention!

Contact:
Prof. Dr. habil. Bernd Blobel, FACMI, FACHI, FHL7, FEFMI
Past-Co-Chair, HL7 Security WG
Past-Chair, EFMI WGs „Security, Safety and Ethics“ and „EHR“
Past-Chair, GDD WG „Privacy and Security in Health and Social Care
University of Regensburg, Medical Faculty
c/o HL7 Germany
An der Schanz 1
50735 Köln
Germany
Email: bernd.blobel@klinik.uni-regensburg.de