Luxemburger Juristische Studien –
Luxembourg Legal Studies

22

Giorgia Bincoletto

Data Protection by Design in the E-Health Care Sector

Theoretical and Applied Perspectives

Nomos

Luxemburger Juristische Studien –
Luxembourg Legal Studies

edited by

Faculty of Law, Economics and Finance
University of Luxembourg

Volume 22

Giorgia Bincoletto

Data Protection by Design in the E-Health Care Sector

Theoretical and Applied Perspectives

Nomos

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

ISBN 978-3-8487-8569-8 (Print)
978-3-7489-2989-5 (ePDF)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN 978-3-8487-8569-8 (Print)
978-3-7489-2989-5 (ePDF)

Library of Congress Cataloging-in-Publication Data
Bincoletto, Giorgia
Data Protection by Design in the E-Health Care Sector
Theoretical and Applied Perspectives
Giorgia Bincoletto
532 pp.
Includes bibliographic references.

ISBN 978-3-8487-8569-8 (Print)
978-3-7489-2989-5 (ePDF)

Onlineversion
Nomos eLibrary

1st Edition 2021

Published by
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Production of the printed version:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-8487-8569-8 (Print)
ISBN 978-3-7489-2989-5 (ePDF)

DOI https://doi.org/10.5771/9783748929895

To my family

Preface

Health care for obvious reasons has become an even more relevant – or at least more publicly discussed – topic in the past two years in the wake of the Covid19-pandemic. Digitalisation and its consequences for all areas of society has been a very much debated topic over the last decade. The combination of health care and digital solutions in that sector has become one of *the* focal points of attention when discussing how to deal with a pandemic of the scale of Covid19. Even though one wished that it would not need such a type of proof for the relevance of finding adequate digital solutions in order to offer more effective services whilst respecting the legal framework and noteably fundamental rights such as the right to privacy, it can be seen as a confirmation of the relevance of the research topic for which you readers are holding the outcome in your hand – or viewing it on a screen respectively.

Giorgia Bincoletto explored in her Ph.D. thesis between the end of 2017 and 2021 a very specific aspect of EU data protection law and how it is relevant in "electronic health care" solutions: "**Data Protection by Design in the E-Health Care Sector: Theoretical and Applied Perspectives**". We are very pleased that with the support of the Faculty of Law of the University of Trento and the "eHealth" Research Units within Fondazione Bruno Kessler and the Competence Center on Digital Health "TrentinoSalute4.0" we are able to bring the results of her thesis to a wider public attention by including this book, based on her thesis, in the "**Luxemburger Juristische Studien – Luxembourg Legal Studies**" with Nomos publisher as volume 22, also available as open access e-book. Digital solutions play a very important role in processing medical information and that in turn is a sensitive category of personal data concerning the patients which are at the same time data subjects. Therefore, it is of utmost importance that such solutions are especially considerate of the requirements to protect and secure the data involved. Not last with its inclusion as a core principle in the EU's General Data Protection Regulation, the concept of Privacy by Design is one of the answers to this challenge. Article 25 of the GDPR sets in its first paragraph the standards that are expected to be met in data processing in this regard, which include technical and organisational measures. *Giorgia Bincoletto* has attempted at analysing more in detail what these requirements mean in practice for solutions in the e-health care

sector. She provides a thorough analysis of the principle and its evolution as well as a very comprehensible overview of data protection issues in the e-health sector. In view of existing standards in the United States of America, to the benefit of European readers, she includes a comparative analysis with those rules. In addition, being an interdisciplinary work, she also gives an overview of technological solutions and tools already in use or being developed, and measures these against the legal framework. With this basis her book can conclude with very concrete guidelines on how to implement data protection by design in e-health record systems, providing guidelines with a kind of checklist that can be used by software developers, data controllers but also any stakeholder involved in this sector. Focusing on e-health record systems allows a very specific answer to the research question which enriches the already very valuable theoretical analysis on which it is based.

The Ph.D. thesis of *Giorgia Bincoletto* was prepared in the framework of the joint international Ph.D. degree programme "Law, Science and Technology" (LAST-JD) of the University of Bologna and in a joint doctorate ("co-tutelle") with the University of Luxembourg. The programme offers an enriching atmosphere that brings together junior researchers on a broad range of topics related to digital matters and encourages an interdisciplinary approach to the research questions tackled. It is a challenging but inspiring task for the students enrolled to not only match this expectation but also conduct their research stays at the partner universities as part of their mobility within the programme. I was privileged to be *Giorgia Bincoletto*'s supervisor of this thesis and could witness how much she profited from the insight and different perspectives of the colleagues involved at the partner universities, both with the professors and research teams as well as with her colleagues in the programme. She was not only active researching her Ph.D. project topic and contributing to the work of my research team during her stay here in Luxembourg, but also published in and presented at international venues and has offered expert insight about Italian data protection authority decisions in the "European Data Protection Law Review". After completing her thesis with the defence on 26th March 2021 at which the jury expressed admiration for the excellent quality of the work, the manuscript was updated for this publication and reflects developments until October 2021. As mentioned in the first lines of this preface, recent events have accelerated the desire and push for e-solutions also in the health care sector. It is obvious that the research topic will move and further evolve in the coming years, but the work published

here will remain of relevance as it offers guidelines that continue to be applicable even if new technological solutions will be developed.

I am convinced that anyone interested in data protection issues generally and even more so specifically in the current state of the e-health sector and specific solutions to creating electronic health record systems, will find this publication valuable and offering concrete solutions. I therefore hope that it will find many readers including potential future junior researchers that understand the value of interdisciplinary research such as the one offered in the LAST-JD-programme. I am also happy to see that *Giorgia Bincoletto* is continuing with the research for which she has laid the basis in her thesis as a post-doctoral researcher at the University of Trento.

Dr. Mark D. Cole
Professor for Media and Telecommunication Law
University of Luxembourg and
Director for Academic Affairs
Institute of European Media Law (EMR)

Acknowledgements

The publication of this work was supported by the Faculty of Law of the University of Trento, the "Health and Wellbeing Impact Area" within Fondazione Bruno Kessler and the Competence Center on Digital Health "TrentinoSalute4.0".

This book is based on the research I carried out during the Ph.D. which continued after the award of the title, and which is still ongoing. Designing technologies with data protection in mind is necessary not only to safeguard personal data, but also to ensure the exercise of other fundamental rights in the digital age.

I would like to acknowledge the professors that guided me along this journey. Prof. Roberto Caso, thank you for your constant support and constructive advice, and for welcoming me in the LawTech Group of the University of Trento, Faculty of Law. Prof. Monica Palmirani, thank you for mentoring me and making everything possible in the Law, Science and Technology Joint Doctorate of the University of Bologna. Prof. Mark David Cole, thank you for your guidance during the period at the University of Luxembourg and for helping me for this publication. My gratitude goes also to Ass. Prof. Paolo Guarda, for his stimulating thinking and advice since university.

I would like to thank all the colleagues and friends from the University of Bologna, the University of Luxembourg and the University of Trento.

Last but not least, I would like to dedicate this book to my family. Special thanks to Niccolò. You always and unconditionally encourage me: our two souls are one.

Table of Contents

List of tables 17

List of figures 19

Abbreviations and Acronyms 21

Chapter 1 Introduction 23

1.1 General introductory remarks 23

1.2 Research methodology and objectives 31

1.3 Structure 34

Chapter 2 Data protection by design: from privacy by design to Article 25 of the GDPR 37

2.1 Introductory remarks 37

2.2 A comparative introduction to privacy by design 38

2.3 A critical analysis of privacy by design 55

2.4 Deconstructing Article 25 of the GDPR 95

2.4.1 Identifying the subjects 105

2.4.2 Defining technical and organisational measures 111

2.4.3 Understanding the state of the art and balancing the costs of implementation 115

2.4.4 Evaluating the nature, scope, context and purposes of data processing 118

2.4.5 Evaluating the risks posed by data processing 120

2.4.6 Defining "appropriate" and "effective" criteria 122

2.4.7 Identifying the time aspect of the requirement 123

2.4.8 Towards the implementation of principles and rights 124

2.4.9 Data protection by default 142

2.5 The related provisions of the GDPR 146

2.5.1 Security measures 147

2.5.2 Data protection impact assessment 150

2.5.3 Certification mechanisms 154

2.6 A comparison between privacy and data protection by design 157
2.7 Balancing the right to data protection against other rights and freedoms 160

Chapter 3 Data protection and the e-health sector 167

3.1 Introductory remarks 167
3.2 Data protection concerns of e-health technologies 168
3.3 Regulatory framework for personal health data 184
3.3.1 The definition of personal health data 196
3.3.1 The legal grounds for processing 203
3.3.3 The relevant and applicable provisions of the GDPR 218
3.4 The case study of Electronic Health Record system 229
3.4.1 The state of the art of EHR 232
3.4.2 The data protection framework for EHRs 243
3.4.3 Cross-border interoperability issues 264
3.5 Balancing the right to data protection against public health 283

Chapter 4 A comparative analysis with the US legal framework 293

4.1 Introductory remarks 293
4.2 Overview of informational privacy in the US and the FIPS 294
4.3 The US legal framework for health informational privacy and for EHRs 313
4.4 Analysing the HIPAA Privacy and Security Rules 335
4.4.1 General requirements 336
4.4.2 The HIPAA Privacy Rule 341
4.4.3 The HIPAA Security Rule 354
4.5 A comparison between HIPAA and DPbD in the e-health context 363

Chapter 5 Technical tools for designing data protection 377

5.1 Introductory remarks 377
5.2 System and software development design 377
5.3 Overview of privacy engineering approaches 385
5.3.1 The PRIPARE project 396
5.3.2 Privacy design strategies 398

5.3.3 LIDDUN methodology 401
5.4 Guidance on the risk assessment framework 403
5.5 Existing standards and PETs for EHR systems 409

Chapter 6 Guidelines for implementing DPbD in the EHR system 421
6.1 Introductory remarks 421
6.2 The methodology of the set of guidelines 422
6.3 Applying DPbD to an EHR system 425
6.3.1 DPbD and the EHR system 425
6.3.2 Technical guidelines and measures 430
6.3.3 Organisational guidelines and measures 438
6.4 The set of guidelines 446
6.5 Notes on liability issues: possible scenarios 458

Chapter 7 Conclusions 469
7.1 Concluding remarks 469
7.2 Open questions 476
7.3 Future research 477

Bibliography 479

Table of Legislation and Cases 527

List of tables

Table 2.1	Classification of the advantages and challenges of PbD	61
Table 2.2	Data protection principles	126
Table 2.3	Data subject's rights	135
Table 2.4	Summary of the comparison between PbD and DPbD	159
Table 3.1	Synthesis of the comparison between GDPR and DPD	215
Table 3.2	Synthesis of the comparison between GDPR and CoE's Rec.	217
Table 3.3	Data subject's rights as a patient	224
Table 3.4	Definitions of ISO/TR 20514:2005	234
Table 3.5	EHR overview: sub-dimensions and functionalities	240
Table 4.1	OECD privacy principles	305
Table 4.2	FTC privacy principles	308
Table 4.3	Summary of the comparison between GDPR grounds and HIPAA rules	348
Table 4.4	GDPR vs. HIPAA rights	372
Table 4.5	Synthesis of the comparison between DPbD and HIPAA	374
Table 5.1	Risk level	405

Table 6.1 DPbD technical guidelines of data at rest before processing 447

Table 6.2 DPbD technical guidelines of data at rest during processing 448

Table 6.3 DPbD technical guidelines of data in use before processing 448

Table 6.4 DPbD technical guidelines of data in use during processing 449

Table 6.5 DPbD technical guidelines of data in transit before processing 450

Table 6.6 DPbD technical guidelines of data in transit during processing 451

Table 6.7 DPbD organisational guidelines before processing 1 451

Table 6.8 DPbD organisational guidelines before processing 2 453

Table 6.9 DPbD organisational guidelines before processing 3 454

Table 6.10 DPbD organisational guidelines data collection 456

Table 6.11 DPbD organisational guidelines during processing 457

List of figures

Figure 3.1 EHR concept overview 242

Figure 3.2 EHR interoperability concept overview 269

Fig. 6.1 DPbD cycle overview 430

Abbreviations and Acronyms

AMA	American Medical Association
CDR	Clinical Data Repository
C.F.R.	Code of Federal Regulations
CIS	Clinical Information System
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPbDf	Data Protection by Default
DPbD	Data Protection by Design
DPO	Data Protection Officer
eHDSI	European e-Health Digital Services Infrastructure
EC	European Commission
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EHR	Electronic Health Record
EMR	Electronic Medical Record
EHDS	European Health Data Space
ENISA	European Union Agency for Network and Information Security
EU	European Union
FIP	Fair Information Practice
FTC	Federal Trade Commission
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
IHE	Integrating the Healthcare Enterprise
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act

HIS	Hospital Information System
HIE	Health Information Exchange
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health Act
HL7	Health Level Seven
ICT	Information and Communication Technologies
IDMS	Identity Management System
IPC	Information Privacy Commissioner
ISO	International Organisation for Standardisation
NHS	National Health Service
OCR	Health and Human Servives' Office for Civil Rights
OECD	Economic Cooperation and Development
ONC	Office of the National Coordinator for Health Information Technology
PII	Personally Identifiable Information
PbD	Privacy by Design
PET	Privacy Enhancing Technology
PHR	Personal Health Record
SMEs	Small and medium-sized enterprises
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
US	United States
VSD	Value Sensitive Design
WHO	World Health Organisation