

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

Table of Contents

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

List of tables

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