

Data Protection and Privacy

The Age of Intelligent Machines

Edited by
Ronald Leenes, Rosamunde van Brakel,
Serge Gutwirth & Paul De Hert



• H A R T •
PUBLISHING

OXFORD AND PORTLAND, OREGON

2017

CONTENTS

<i>Preface</i>	v
<i>List of Contributors</i>	xiii
1. EU Data Protection and ‘Treaty-base Games’: When Fundamental Rights are Wearing Market-making Clothes.....	1
<i>Laima Jančiūtė</i>	
I. Introduction	1
A. The Case for this Study	1
B. Policy Outcomes of the Rights-based and Market-oriented Approaches	2
C. Political Pragmatism and the Early History of Fundamental Rights in the EU	4
II. Rational Choice and Historical Institutionalism.....	5
III. The CJEU: Filling the Gap, but Why and How Far? Tracing Strategic Interests of the Constitutional Court	8
A. The Early Challenges to the CJEU Authority.....	8
B. The Challenges to the CJEU Status Quo in the Post-Lisbon Era	9
C. The Member States and the CJEU’s Strategic Interests	11
D. Parameter-setting.....	12
IV. The Charter—A Victim of Domestic Politics?.....	13
A. EU Integration in the Field of Civic Interests.....	13
B. The Charter and the Member States’ Sovereignty Concerns.....	14
V. Directive 95/46/EC, GDPR, and the Market Imprint.....	17
A. ‘Treaty-base Games’: Explaining the Market-framing of the EU First Data Protection Instrument.....	17
B. The Development of the EU Data Protection Law and the Market-framing Implications	20
VI. Conclusions	25
References.....	26
2. The ‘Risk Revolution’ in EU Data Protection Law: We can’t Have Our Cake and Eat it, Too.....	33
<i>Claudia Quelle</i>	
I. Introduction	34
II. The Role of ‘Risk’ in the Risk-Based Approach	37

III.	‘Risk’ and the Legal Obligations in the GDPR.....	42
A.	The Link between ‘Theory’ and ‘Practice’.....	42
B.	‘Taking into Account’ the Risks.....	44
i.	Scalable Compliance Measures.....	44
ii.	Substantive Protection against Risks.....	45
iii.	The Limits to Enforcement Action against Risk-Taking.....	50
C.	The Risk-Based Approach and Legal Compliance.....	52
IV.	Were the Data Protection Principles and the Data Subject Rights Risk-Based to Start With?.....	53
A.	Obligations which Require a Risk-Oriented Result	54
B.	Obligations which Require a Risk-Oriented Effort.....	56
C.	Obligations which Are not Risk-Oriented.....	56
D.	The Discretion of Controllers vs the Control Rights of Data Subjects.....	58
V.	Conclusion.....	59
	References.....	60
3.	No Privacy without Transparency	63
	<i>Roger Taylor</i>	
I.	Introduction	63
II.	Describing the Harms from Loss of Privacy	64
A.	Public Perceptions of the Privacy Related Harm	65
B.	Insecure Use and Imprecise Use of Data	68
III.	How Does Data Protection Protect against Insecure and Imprecise Use of Data?.....	71
A.	The GDPR	72
B.	Transparency, Consent and Fair Processing.....	74
C.	Privacy vs Consumer Protection.....	76
IV.	Measuring the Benefits and Risks of Data-driven Automated Decision-making (Surveillance).....	77
A.	Model Surveillance System.....	78
B.	Estimating the Net Benefit of a Surveillance System.....	79
C.	Risks of Surveillance Systems Resulting in Net Harm	80
V.	How Might Regulators Ensure Reliable Information about the Impact of Surveillance Systems be Generated?.....	81
A.	Ownership of Data	83
VI.	Conclusion.....	84
	References.....	85
4.	Machine Learning with Personal Data	89
	<i>Dimitra Kamarinou, Christopher Millard and Jatinder Singh</i>	
I.	Introduction	89
II.	Lawfulness	93
A.	Profiling as a Type of Processing.....	93
i.	The Elements of the Profiling Process	94

B.	The Decision and its Effects.....	97
C.	Data Protection Impact Assessments (DPIA).....	99
D.	Derogations from the Rule	101
E.	Potential Consequences of Non-Compliance.....	102
III.	Fairness	103
IV.	Transparency	106
V.	Conclusions	110
	References.....	112
5.	Bridging Policy, Regulation and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR.....	115
	<i>Runshan Hu, Sophie Stalla-Bourdillon, Mu Yang, Valeria Schiavo and Vladimiro Sassone</i>	
I.	Introduction	115
II.	The Three Types of Data.....	119
A.	The GDPR Definitions.....	119
i.	Additional Information	121
ii.	Direct and Indirect Identifiers	122
iii.	Data Sanitisation Techniques	123
iv.	Contextual Controls	123
B.	Re-Identification Risks.....	124
III.	A Risk-based Analysis of the Three Types of Data	125
A.	Local, Global and Domain Linkability.....	125
B.	Anonymised Data	126
C.	Pseudonymised Data.....	126
D.	Art. 11 Data.....	128
IV.	Data Sanitisation Techniques and Contextual Controls	130
A.	Effectiveness of Data Sanitisation Techniques	130
B.	Improving Data Utility with Contextual Controls.....	134
C.	Improving Data Utility with Dynamic Sanitisation Techniques and Contextual Controls	139
V.	Conclusion.....	140
	References.....	141
6.	Are We Prepared for the 4th Industrial Revolution? Data Protection and Data Security Challenges of Industry 4.0 in the EU Context	143
	<i>Carolin Moeller</i>	
I.	Introduction	143
II.	Defining IND 4.0—The Regulatory Use and Key Features of a Sui Generis Concept	145
A.	IND 4.0 as a Regulatory Tool and as a Sui Generis Concept	145
B.	Conceptual Features of IND 4.0	147
III.	Data Protection Challenges of IND 4.0 and the EU Legal Context....	149
A.	Data Protection Challenges in regard to Customer Data in the IND 4.0 Context.....	149

B.	Data Protection Challenges in relation to Employee Data in an IND 4.0 Context.....	155
IV.	Data Security Challenges of IND 4.0 and the EU Legal Context.....	159
V.	Conclusion.....	163
	References.....	164
7.	Reasonable Expectations of Data Protection in Telerehabilitation— A Legal and Anthropological Perspective on Intelligent Orthoses	167
	<i>Martina Klausner and Sebastian Golla</i>	
I.	Introduction	167
A.	Telerehabilitation: A Challenge for Data Protection	167
B.	Research Context and Methods.....	168
C.	Research Focus: The Orthoses Project.....	169
II.	The Legal Angle: Reasonable Expectations and Privacy by Design	170
A.	Reasonable Expectations and Privacy by Design in the GDPR.....	171
B.	Gaining Legal Certainty with ‘Katz Content’	172
C.	Reasonable Expectations and the Use of Intelligent Systems in Telerehabilitation	174
III.	The Anthropological Angle: Reasonable Expectations of Minors in Brace Therapy	176
A.	Methods and Overview of Findings.....	176
B.	Analytical Framework: The Concept of ‘Territories of the Self’ (Erving Goffman)	177
C.	Discussion of Empirical Findings.....	180
i.	Attitudes Regarding Data Sharing.....	181
a)	Minimization of Data Disclosure	181
b)	Data-Sharing as Trade-Off	181
c)	Impracticality of Controlling Personal Data.....	182
d)	Data-Sharing without Concern	182
ii.	Information Preserves Concerning ‘Data Especially Worthy of Protection’	182
iii.	Attitudes and Expectations of Handling Data Concerning Health.....	184
IV.	Conclusion.....	187
	References.....	189
8.	Considering the Privacy Design Issues Arising from Conversation as Platform	193
	<i>Ewa Luger and Gilad Rosner</i>	
I.	Introduction	193
II.	Conversation as Platform	196
III.	The Privacy Impact of Sensed Conversation; A Focus on Child-Facing Technology	199
A.	Privacy of Child and Adult Communications	200
B.	Privacy of Children’s Play.....	201

C. Inappropriate Use	201
D. Introduction of Third Parties.....	202
IV. The Problem of Intelligent Systems.....	202
A. Learning, Error and the Importance of Social Context.....	204
B. Opacity, Comprehension and Informing.....	205
C. User Consent	207
V. Conclusions and Recommendations.....	208
A. Rethinking the Design of Consent Mechanism for Conversational Systems	209
B. Create New Boundary Objects and Privacy Grammars to Support User Understanding and Trust	210
C. Undertake Research on the Potential Increase and Normalisation of Child Surveillance	210
References.....	211
9. Concluding remarks at the 10th Computers, Privacy and Data Protection Conference: 27 January 2017.....	213
<i>Giovanni Buttarelli</i>	
<i>Index</i>	219