Binding Corporate Rules

Corporate Self-Regulation of Global Data Transfers

LOKKE MOEREL

OXFORD UNIVERSITY PRESS
## Contents

Table of Cases .......................... xiii
Table of Instruments, International Agreements, and Guidelines xiv
List of Abbreviations .................. xxi

1. Introduction .......................... 1
   1.1 Background .......................... 1
   1.2 Subject Matter and Aim of this Book 8
      1.2.1 Background .......................... 9
      1.2.2 Aim of this book ....................... 11
      1.2.3 Relevance and recommendations 12
      1.2.4 Prior research and publications 13
      1.2.5 Scope ............................... 15
   1.3 Outline ............................. 15

2. Binding Corporate Rules: An Overview 18
   2.1 Data Here, Data There, Data Everywhere 18
   2.2 Relevance of BCR as a Data Transfer Tool at Global Level 24
      2.2.1 No global standard ..................... 25
      2.2.2 Bridging function of BCR between different legal systems 26
      2.2.3 Limitations of state legislative and enforcement powers 28
      2.2.4 Stepping stone to further harmonization 31
   2.3 Evaluation of the BCR Regime from Different Dimensions 32
      2.3.1 Evaluation of BCR as a form of transnational private regulation 33
      2.3.2 Evaluation of BCR as implementation of corporate accountability 33
      2.3.3 Evaluation of BCR in the context of corporate social responsibility 34
   2.4 The Quest for Meta-norms for BCR 35

3. The Worldwide Data Protection Regulatory Landscape 37
   3.1 EU Data Protection Regime 37
      3.1.1 Material processing principles ........... 39
      3.1.2 Other fundamental obligations ........... 40
      3.1.3 Rights of data subjects .................. 41
      3.1.4 Scope of applicability ................... 41
      3.1.5 EU transfer rules ........................ 43
      3.1.6 Third-party processors ................. 47
      3.1.7 Jurisdiction and enforcement ............ 48
      3.1.8 Working Party 29 ........................ 54
      3.1.9 Self- and co-regulation ................... 56
Contents

3.2 Other Comprehensive Regimes 57
3.3 Limited Regimes 58
3.4 APEC Privacy Framework 58

4. Trends and Developments in the Legal Landscape 61
4.1 Increasing Tension between Different Regulatory Systems 61
4.2 Towards a Global Standard for Data Protection? 63
4.3 Cross-border Enforcement Issues 68
4.4 Thinking about Alternative Solutions for Enforcement 74
  4.4.1 Self-regulation backed up by governmental enforcement tools 74
  4.4.2 Parallel with enforcement of consumer protection laws 75
  4.4.3 Country of origin approach 80
  4.4.4 Accountability approach 85
  4.4.5 Private choice of law and forum in transnational private regulation 86

5. Trends and Developments in Multinational Corporate Practice 87
5.1 Increase in International Data Transfers within and between Multinationals 87
5.2 Multiple Jurisdictions 88
5.3 Corporate Mitigation of Data Protection Risks 91
5.4 Other Drivers for Corporate Privacy Policies 94

6. The BCR Regime 100
6.1 Introduction 100
6.2 BCR Requirements 101
6.3 Different Types of BCR
  6.3.1 BCR for controllers 105
  6.3.2 BCR for employee data vs BCR for customer data 106
  6.3.3 BCR for processors 106
6.4 EU BCR Approval Procedure 108
  6.4.1 How to align the MRP with EU works council requirements? 109
6.5 Shortcomings of the BCR Approval Procedure 111
6.6 How to Address Shortcomings in the BCR Regime and the BCR Approval Procedure?
  6.6.1 Recognize BCR, define main BCR requirements, and impose the Mutual Recognition Procedure 113
  6.6.2 Define BCR requirements in general principles 117
  6.6.3 Adequate level of protection 118
  6.6.4 Harmonize the powers of DPAs 119
  6.6.5 Replace Directive by an EU regulation 120
  6.6.6 Role of the Working Party 29 121
6.7 Recognition of BCR in Other Countries 127
6.8 Conclusion 130
Contents

7. BCR and Contract Law 131
   7.1 Introduction 131
   7.2 Internally Binding 132
      7.2.1 Binding on group companies 132
      7.2.2 Binding on employees 132
   7.3 Externally Binding 132
      7.3.1 Enforceability of unilateral undertakings 132
      7.3.2 Other grounds of enforcement 133
      7.3.3 Grounds of enforcement in the EU 134
      7.3.4 Enforcement of corporate data protection policies in the US 135
      7.3.5 Solutions to ensure that BCR are externally binding 136
   7.4 Contractual 'Supply Chain Management' 137
   7.5 How to Address the Contractual Supply Chain Management Issues in BCR? 139
      7.5.1 Enforceability against the external supplier 139
      7.5.2 Enforceability against the multinational 141
      7.5.3 From 'supply chain' to 'network' 143
   7.6 Conclusion as to Contractual Issues of BCR 144
8. BCR and EU Rules of Private International Law 145
   8.1 Introduction 145
      8.1.1 PIL as a mechanism 146
      8.1.2 Preferences of multinationals 147
      8.1.3 Preferences of beneficiaries of BCR? 147
   8.2 Applicability, Jurisdiction, and Enforcement 148
   8.3 Role Left for EU Rules of PIL? 149
      8.3.1 Qualification of data protection law 149
      8.3.2 Do the conflict rules of the Directive take precedence over PIL? 151
      8.3.3 Choice of law and forum 152
   8.4 The Applicability, Supervision, and Enforcement Regime of BCR: How It May Work 159
      8.4.1 How should the applicable law regime be set up under BCR? 160
      8.4.2 How should the enforcement regime for BCR be set up? 161
      8.4.3 How should supervision of BCR be set up? 161
   8.5 Choice of Law and Forum 162
      8.5.1 Employee contracts 162
      8.5.2 Consumer contracts 163
   8.6 Relevance of Rome I and the Brussels I Regulation for BCR 163
      8.6.1 Contract concluded 165
      8.6.2 Matters relating to a contract 167
      8.6.3 Application of ECJ case law to BCR 167
      8.6.4 Relevance of Rome II? 169
8.7 Summary Conclusion: Applicability of Employee and Consumer Protection Regimes 170
8.8 Are the Choice of Law and Forum Clauses Validly Entered Into? 171
8.9 Are the Choice of Law and Forum Clauses Themselves Valid and Binding? 171
8.10 Choice of Forum should be (Evidenced) in Writing 172
  8.10.1 BCR as unilateral undertakings 172
  8.10.2 Contractual solution 173
8.11 Conclusions: How the Applicability, Supervision, and Enforcement Regime of BCR May Work 174

9. BCR and the 'Accountability Principle'
9.1 The Accountability Principle in the Field of Data Protection 175
9.2 The Accountability Principle According to General Literature 178
  9.2.1 External disclosure requirement 180
  9.2.2 Learning-oriented approach 181
  9.2.3 Sticks and carrots 184
  9.2.4 The 'right' regulatory response 186
9.3 Review of the BCR Regime against Accountability Requirements in the General Literature 186
  9.3.1 Good fit with data protection 186
  9.3.2 Learning-oriented approach 188
  9.3.3 External disclosure requirement 190
  9.3.4 Sticks and carrots 190
9.4 The Accountability Principle in the Field of Data Protection 193
  9.4.1 Working Party 29 accountability requirements 194
  9.4.2 Proposed Regulation accountability requirements 202
  9.4.3 Madrid accountability requirements 204
  9.4.4 Centre for Information Policy Leadership accountability requirements 206
9.5 Accountability for Onward Data Transfers in BCR? 209
  9.5.1 Define the core principles only 214
  9.5.2 Focus on alternative means of redress 214
  9.5.3 Conclusion and starting points for core principles 215
9.6 Solution of Working Party 29 to Achieve Joint Responsibility of Controller and Processor 219
9.7 Proposal of the Working Party 29 to Introduce Accountability for Onward Data Transfers 224
9.8 Conclusion as to Accountability 227

10. BCR as a Form of Transnational Private Regulation 228
10.1 Rules for Rule-making 228
10.2 Criteria for Evaluating Public Law 230
10.3 Different Levels of Norm-setting for BCR
10.3.1 Actors involved in the BCR norm-setting process 232
10.3.2 Stakeholders in the BCR norm-setting process 233
10.4 General Starting Points for 'Privatization' of Criteria for Evaluating Public Law
10.4.1 Enhanced accountability 234
10.4.2 Empirical research 236
10.4.3 Normative criteria 237
10.4.4 Relative lack of legitimacy 237
10.5 TPR Regulating Human Rights
10.5.1 Introduction 238
10.5.2 Rationale 239
10.5.3 TPR of data protection 244
10.5.4 BCR 247
10.6 The Concept of Legitimacy: The Normative Perspective
10.6.1 General introduction 248
10.6.2 Normative criteria 249
10.6.3 Accountability as a virtue 250
10.6.4 Accountability as a mechanism 252
10.6.5 Cumulative overview accountability requirements 255
10.7 Are BCR Legitimate?: The Normative Perspective
10.7.1 Identifying the actors and accountability forums involved in the three phases 255
10.7.2 Phase (a) BCR norm-setting by the Working Party 29 257
10.7.3 Accountability ex ante Working Party 29 258
10.7.4 Accountability ex post Working Party 29 264
10.7.5 Phase (a) norm-setting by a Lead DPA in respect of individual BCR 265
10.7.6 Accountability ex post: phase (b) monitoring and evaluation and phase (c) enforcement 269
10.8 Visualization Proposals 273
10.9 Conclusion as to Legitimacy of BCR as a Form of TPR 275

11. BCR and Corporate Social Responsibility
11.1 Norms Regulating CSR 277
11.2 CSR and International Law
11.2.1 Introduction 278
11.2.2 Do the core CSR principles include data protection? 279
11.2.3 OECD Guidelines 280
11.2.4 UN Global Compact 281
11.2.5 Draft UN Norms 2003 281
11.2.6 ILO's Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy 282
11.2.7 EU position on CSR 283
11.2.8 The Ruggie Framework for future action 284
11.2.9 Due diligence 286
11.2.10 CSR and the trust game 289
11.2.11 CSR of human rights 290

12. Conclusion 291
12.1 Hypotheses 294
12.2 Re-(i) Avoiding Gaps in Data Protection 294
12.3 Re (ii) Avoiding Gaps in Enforcement 294
12.4 Re (iii) Improved Regulation of Transborder Data Flows 295

Appendix 1: Overview of Recommendations to EU Legislators 297
Appendix 2: BCR for Employee Data 301
Appendix 3: BCR for Customer Data 321
Index 343