

# CONTENTS

**LIST OF CONTRIBUTORS . . . . . XIV**

**FOREWORD TO THE THIRD EDITION . . . . . XVIII**  
*by Christopher Kuner*

**FOREWORD TO THE FIRST AND SECOND EDITIONS . . . . . XIX**  
*by Jean-Philippe Walter*

**ACKNOWLEDGEMENTS . . . . . XXI**

**GLOSSARY OF DEFINED TERMS AND ABBREVIATIONS . . . . . XXIV**

**1 INTRODUCTION . . . . . 3**

1.1 Background . . . . . 4

1.2 Objective . . . . . 4

1.3 Structure and approach . . . . . 8

1.4 Target audience . . . . . 9

**PART I: DATA PROTECTION PRINCIPLES IN HUMANITARIAN ACTION . . . . . 11**  
*Massimo Marelli*

**2 BASIC PRINCIPLES OF DATA PROTECTION . . . . . 13**

2.1 Introduction . . . . . 14

2.2 Basic data protection concepts . . . . . 16

2.3 Aggregate, Pseudonymized and Anonymized data sets . . . . . 18

2.4 Applicable law and International Organizations . . . . . 20

2.5 Data Processing principles . . . . . 21

2.5.1 The principle of the fairness and lawfulness of Processing . . . . . 21

2.5.2 The purpose limitation principle . . . . . 22

2.5.3 The principle of proportionality . . . . . 24

2.5.4 The principle of data minimization . . . . . 26

2.5.5 The principle of data quality . . . . . 27

2.6 Special Data Processing situations . . . . . 27

2.6.1 Health purposes . . . . . 27

2.6.2 Administrative activities . . . . . 28

2.7 Data retention . . . . . 28

2.8 Data security and Processing security . . . . . 29

2.8.1 Introduction . . . . . 29

2.8.2 Physical security . . . . . 31

|          |                                                                  |           |
|----------|------------------------------------------------------------------|-----------|
| 2.8.3    | IT security . . . . .                                            | 31        |
| 2.8.4    | Duty of discretion and staff conduct . . . . .                   | 32        |
| 2.8.5    | Contingency planning . . . . .                                   | 33        |
| 2.8.6    | Destruction methods . . . . .                                    | 33        |
| 2.8.7    | Other measures . . . . .                                         | 34        |
| 2.9      | The principle of accountability . . . . .                        | 35        |
| 2.10     | Information . . . . .                                            | 35        |
| 2.10.1   | Data collected from the Data Subject . . . . .                   | 36        |
| 2.10.2   | Information notices . . . . .                                    | 36        |
| 2.10.3   | Data not collected from the Data Subject . . . . .               | 37        |
| 2.11     | Rights of Data Subjects . . . . .                                | 38        |
| 2.11.1   | Introduction . . . . .                                           | 38        |
| 2.11.2   | Access . . . . .                                                 | 38        |
| 2.11.3   | Correction . . . . .                                             | 40        |
| 2.11.4   | Right to erasure . . . . .                                       | 40        |
| 2.11.5   | Right to object . . . . .                                        | 41        |
| 2.12     | Data sharing and International Data Sharing . . . . .            | 41        |
| <b>3</b> | <b>LEGAL BASES FOR PERSONAL DATA PROCESSING . . . . .</b>        | <b>43</b> |
| 3.1      | Introduction . . . . .                                           | 44        |
| 3.2      | Consent . . . . .                                                | 45        |
| 3.2.1    | Unambiguous . . . . .                                            | 46        |
| 3.2.2    | Timing . . . . .                                                 | 46        |
| 3.2.3    | Validity . . . . .                                               | 46        |
| 3.2.4    | Vulnerability . . . . .                                          | 46        |
| 3.2.5    | Children . . . . .                                               | 47        |
| 3.2.6    | Informed . . . . .                                               | 48        |
| 3.2.7    | Documented . . . . .                                             | 48        |
| 3.2.8    | Withholding/Withdrawing Consent . . . . .                        | 48        |
| 3.3      | Vital interest . . . . .                                         | 49        |
| 3.4      | Important grounds of public interest . . . . .                   | 50        |
| 3.5      | Legitimate interest . . . . .                                    | 51        |
| 3.6      | Performance of a contract . . . . .                              | 52        |
| 3.7      | Compliance with a legal obligation . . . . .                     | 53        |
| 3.7.1    | The disclosure of Personal Data to authorities . . . . .         | 54        |
| <b>4</b> | <b>INTERNATIONAL DATA SHARING . . . . .</b>                      | <b>57</b> |
| 4.1      | Introduction . . . . .                                           | 58        |
| 4.2      | Basic rules for International Data Sharing . . . . .             | 59        |
| 4.3      | Providing a legal basis for International Data Sharing . . . . . | 60        |
| 4.3.1    | Introduction . . . . .                                           | 60        |
| 4.3.2    | Legal bases for International Data Sharing . . . . .             | 60        |

| CONTENTS                                                                                        | vii       |
|-------------------------------------------------------------------------------------------------|-----------|
| 4.4 Mitigating the risks to the individual . . . . .                                            | 61        |
| 4.4.1 Appropriate safeguards/Contractual clauses . . . . .                                      | 61        |
| 4.4.2 Accountability . . . . .                                                                  | 63        |
| 4.5 Data Controller/Data Processor relationship . . . . .                                       | 63        |
| <b>5 DATA PROTECTION IMPACT ASSESSMENTS (DPIAS) . . . . .</b>                                   | <b>65</b> |
| 5.1 Introduction . . . . .                                                                      | 66        |
| 5.2 The DPIA process . . . . .                                                                  | 67        |
| 5.2.1 Is a DPIA necessary? . . . . .                                                            | 67        |
| 5.2.2 The DPIA team . . . . .                                                                   | 67        |
| 5.2.3 Describing the Processing of Personal Data . . . . .                                      | 68        |
| 5.2.4 Consulting stakeholders . . . . .                                                         | 68        |
| 5.2.5 Identify risks . . . . .                                                                  | 69        |
| 5.2.6 Assess the risks . . . . .                                                                | 69        |
| 5.2.7 Identify solutions . . . . .                                                              | 70        |
| 5.2.8 Propose recommendations . . . . .                                                         | 72        |
| 5.2.9 Implement the agreed recommendations . . . . .                                            | 72        |
| 5.2.10 Provide expert review and/or audit of the DPIA . . . . .                                 | 73        |
| 5.2.11 Update the DPIA if there are changes in the project . . . . .                            | 73        |
| <b>PART II: SPECIFIC PROCESSING SITUATIONS, TECHNOLOGIES AND TECHNOLOGY AREAS . . . . .</b>     | <b>75</b> |
| <b>6 DESIGNING FOR DATA PROTECTION . . . . .</b>                                                | <b>77</b> |
| <i>Carmela Troncoso and Wouter Lueks</i>                                                        |           |
| 6.1 Introduction . . . . .                                                                      | 78        |
| 6.1.1 What is a system? . . . . .                                                               | 79        |
| 6.2 Case study: Privacy-preserving contact-tracing apps . . . . .                               | 79        |
| 6.2.1 Decentralized privacy-preserving proximity tracing . . . . .                              | 81        |
| 6.3 Protection of individuals and their dignity and rights through purpose limitation . . . . . | 82        |
| 6.3.1 Why determining purpose matters . . . . .                                                 | 84        |
| 6.3.2 Determining purpose . . . . .                                                             | 87        |
| 6.3.3 Analysing purpose limitation . . . . .                                                    | 88        |
| 6.4 The role of data minimization . . . . .                                                     | 93        |
| 6.5 Challenges to purpose limitation . . . . .                                                  | 94        |
| <b>7 DRONES/UAVS AND REMOTE SENSING . . . . .</b>                                               | <b>97</b> |
| <i>Massimo Marelli</i>                                                                          |           |
| 7.1 Introduction . . . . .                                                                      | 98        |
| 7.2 Application of basic data protection principles . . . . .                                   | 101       |
| 7.2.1 Legal bases for Personal Data Processing . . . . .                                        | 102       |
| 7.2.2 Transparency/Information . . . . .                                                        | 104       |

|          |                                                           |            |
|----------|-----------------------------------------------------------|------------|
| 7.2.3    | Purpose limitation and Further Processing . . . . .       | 105        |
| 7.2.4    | Data minimization . . . . .                               | 105        |
| 7.2.5    | Data retention . . . . .                                  | 106        |
| 7.2.6    | Data security . . . . .                                   | 106        |
| 7.3      | Rights of Data Subjects . . . . .                         | 106        |
| 7.4      | Data sharing . . . . .                                    | 108        |
| 7.5      | International Data Sharing . . . . .                      | 109        |
| 7.6      | Data Controller/Data Processor relationship . . . . .     | 109        |
| 7.7      | Data Protection Impact Assessments . . . . .              | 110        |
| <b>8</b> | <b>BIOMETRICS . . . . .</b>                               | <b>113</b> |
|          | <i>Massimo Marelli</i>                                    |            |
| 8.1      | Introduction . . . . .                                    | 114        |
| 8.2      | Application of basic data protection principles . . . . . | 116        |
| 8.2.1    | Legal bases for Personal Data Processing . . . . .        | 118        |
| 8.2.2    | Fair and lawful Processing . . . . .                      | 120        |
| 8.2.3    | Purpose limitation and Further Processing . . . . .       | 121        |
| 8.2.4    | Data minimization . . . . .                               | 122        |
| 8.2.5    | Data retention . . . . .                                  | 123        |
| 8.2.6    | Data security . . . . .                                   | 123        |
| 8.2.7    | Excessiveness by nature . . . . .                         | 124        |
| 8.3      | Rights of Data Subjects . . . . .                         | 124        |
| 8.4      | Data sharing . . . . .                                    | 125        |
| 8.5      | International Data Sharing . . . . .                      | 125        |
| 8.6      | Data Controller/Data Processor relationship . . . . .     | 126        |
| 8.7      | Data Protection Impact Assessments . . . . .              | 126        |
| <b>9</b> | <b>CASH AND VOUCHER ASSISTANCE . . . . .</b>              | <b>129</b> |
|          | <i>Massimo Marelli</i>                                    |            |
| 9.1      | Introduction . . . . .                                    | 130        |
| 9.2      | Application of basic data protection principles . . . . . | 134        |
| 9.3      | Basic principles of data protection . . . . .             | 135        |
| 9.3.1    | Legal bases for Personal Data Processing . . . . .        | 136        |
| 9.3.2    | Purpose limitation and Further Processing . . . . .       | 137        |
| 9.3.3    | Data minimization . . . . .                               | 139        |
| 9.3.4    | Data retention . . . . .                                  | 140        |
| 9.3.5    | Data security . . . . .                                   | 140        |
| 9.4      | Rights of Data Subjects . . . . .                         | 141        |
| 9.5      | Data sharing . . . . .                                    | 141        |
| 9.6      | International Data Sharing . . . . .                      | 142        |
| 9.7      | Data Controller/Data Processor relationship . . . . .     | 143        |
| 9.8      | Data Protection Impact Assessments . . . . .              | 143        |

**10 CLOUD SERVICES . . . . . 147**

*Paolo Balboni*

10.1 Introduction . . . . . 148

10.2 Data Controller/Data Processor relationship . . . . . 151

10.3 Responsibility and accountability in the cloud . . . . . 151

10.4 Application of basic data protection principles . . . . . 152

    10.4.1 Legal bases for Personal Data Processing . . . . . 152

    10.4.2 Fair and lawful Processing . . . . . 153

    10.4.3 Purpose limitation and Further Processing . . . . . 153

    10.4.4 Transparency . . . . . 154

    10.4.5 Data retention . . . . . 155

10.5 Data security . . . . . 156

    10.5.1 Data in transit protection . . . . . 160

    10.5.2 Asset protection . . . . . 160

    10.5.3 Separation between users . . . . . 162

    10.5.4 Governance . . . . . 162

    10.5.5 Operational security . . . . . 162

    10.5.6 Personnel . . . . . 163

    10.5.7 Development . . . . . 163

    10.5.8 Supply chain . . . . . 163

    10.5.9 User management . . . . . 163

    10.5.10 Identity and authentication . . . . . 164

    10.5.11 External interfaces . . . . . 164

    10.5.12 Service administration . . . . . 164

    10.5.13 Audits . . . . . 164

    10.5.14 Service usage . . . . . 164

10.6 Rights of Data Subjects . . . . . 165

10.7 International Data Sharing . . . . . 165

10.8 Data Protection Impact Assessments . . . . . 165

10.9 Privileges and immunities and the cloud . . . . . 166

    10.9.1 Legal measures . . . . . 166

    10.9.2 Organizational measures . . . . . 167

    10.9.3 Technical measures . . . . . 167

10.10 Codes of conduct . . . . . 167

**11 CLOUD AND GOVERNMENT ACCESS . . . . . 171**

*Andrea Raab-Gray*

11.1 Mapping legislations allowing governments to require service providers to disclose Humanitarian Data . . . . . 173

    11.1.1 Legal frameworks allowing governments to compel service providers to disclose humanitarian data for purposes of national security . . . . . 174

|                                   |                                                                                                                                                                   |            |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 11.1.2                            | Legal frameworks allowing governments to compel service providers to disclose data for purposes of criminal proceedings . . . . .                                 | 178        |
| 11.2                              | Impacts of compelled disclosure on Humanitarian Action and persons benefiting from it . . . . .                                                                   | 184        |
| 11.3                              | Mitigating the risk of disclosure of Humanitarian Data processed in a public cloud environment . . . . .                                                          | 186        |
| 11.3.1                            | Ensuring the effectiveness of privileges and immunities . . . . .                                                                                                 | 186        |
| 11.3.2                            | Sensitizing States to the importance of not using or requesting Humanitarian Data for purposes incompatible with the work of Humanitarian Organizations . . . . . | 189        |
| <b>12</b>                         | <b>MOBILE MESSAGING APPS . . . . .</b>                                                                                                                            | <b>191</b> |
| <i>Lina Jasmontaite-Zaniewicz</i> |                                                                                                                                                                   |            |
| 12.1                              | Introduction . . . . .                                                                                                                                            | 192        |
| 12.1.1                            | Mobile messaging apps in Humanitarian Action . . . . .                                                                                                            | 194        |
| 12.2                              | Application of basic data protection principles . . . . .                                                                                                         | 195        |
| 12.2.1                            | Processing of Personal Data through mobile messaging apps . . . . .                                                                                               | 196        |
| 12.2.2                            | What kind of data do messaging apps collect or store? . . . . .                                                                                                   | 197        |
| 12.2.3                            | How could other parties access data shared on messaging apps? . . . . .                                                                                           | 200        |
| 12.2.4                            | Messaging app features related to privacy and security . . . . .                                                                                                  | 202        |
| 12.2.5                            | Processing of Personal Data collected through mobile messaging apps . . . . .                                                                                     | 205        |
| 12.3                              | Legal bases for Personal Data Processing . . . . .                                                                                                                | 206        |
| 12.4                              | Data retention . . . . .                                                                                                                                          | 207        |
| 12.5                              | Data Subject rights to rectification and deletion . . . . .                                                                                                       | 207        |
| 12.6                              | Data minimization . . . . .                                                                                                                                       | 208        |
| 12.7                              | Purpose limitation and Further Processing . . . . .                                                                                                               | 209        |
| 12.8                              | Managing, analysing and verifying data . . . . .                                                                                                                  | 209        |
| 12.9                              | Data protection by design . . . . .                                                                                                                               | 210        |
| 12.10                             | International Data Sharing . . . . .                                                                                                                              | 211        |
| <b>13</b>                         | <b>DIGITAL IDENTITY . . . . .</b>                                                                                                                                 | <b>213</b> |
| <i>Vincent Graf Narbel</i>        |                                                                                                                                                                   |            |
| 13.1                              | Introduction . . . . .                                                                                                                                            | 214        |
| 13.1.1                            | Authentication, identification and verification: Who are you and how can you prove it? . . . . .                                                                  | 216        |
| 13.1.2                            | Digital Identity . . . . .                                                                                                                                        | 217        |
| 13.1.3                            | System design and governance . . . . .                                                                                                                            | 218        |
| 13.1.4                            | Digital Identity in the humanitarian sector: Possible scenarios . . . . .                                                                                         | 220        |
| 13.1.5                            | Digital Identity as foundational identity . . . . .                                                                                                               | 221        |
| 13.2                              | Data Protection Impact Assessments . . . . .                                                                                                                      | 222        |
| 13.3                              | Data protection by design and by default . . . . .                                                                                                                | 222        |

|           |                                                               |            |
|-----------|---------------------------------------------------------------|------------|
| 13.4      | Data Controller/Data Processor relationship . . . . .         | 223        |
| 13.5      | Rights of Data Subjects . . . . .                             | 224        |
| 13.5.1    | Right of access . . . . .                                     | 225        |
| 13.5.2    | Rights to rectification and erasure . . . . .                 | 226        |
| 13.6      | Application of basic data protection principles . . . . .     | 226        |
| 13.6.1    | Legal bases for Personal Data Processing . . . . .            | 226        |
| 13.6.2    | Purpose limitation and Further Processing . . . . .           | 227        |
| 13.6.3    | Proportionality . . . . .                                     | 227        |
| 13.6.4    | Data minimization . . . . .                                   | 228        |
| 13.6.5    | Data security . . . . .                                       | 228        |
| 13.6.6    | Data retention . . . . .                                      | 229        |
| 13.7      | International Data Sharing . . . . .                          | 229        |
| <b>14</b> | <b>SOCIAL MEDIA . . . . .</b>                                 | <b>231</b> |
|           | <i>Júlia Zomignani Barboza and Lina Jasmontaite-Zaniewicz</i> |            |
| 14.1      | Introduction . . . . .                                        | 232        |
| 14.1.1    | Social media in the humanitarian sector . . . . .             | 232        |
| 14.1.2    | Social media and data . . . . .                               | 234        |
| 14.2      | Data Protection Impact Assessments . . . . .                  | 239        |
| 14.3      | Ethical issues and other challenges . . . . .                 | 241        |
| 14.4      | Data Controller/Data Processor relationship . . . . .         | 243        |
| 14.5      | Basic data protection principles . . . . .                    | 244        |
| 14.5.1    | Legal bases for Personal Data Processing . . . . .            | 244        |
| 14.5.2    | Information . . . . .                                         | 245        |
| 14.5.3    | Data retention . . . . .                                      | 246        |
| 14.5.4    | Data security . . . . .                                       | 247        |
| 14.6      | International Data Sharing . . . . .                          | 247        |
| <b>15</b> | <b>BLOCKCHAIN . . . . .</b>                                   | <b>249</b> |
|           | <i>Vincent Graf Narbel</i>                                    |            |
| 15.1      | Introduction . . . . .                                        | 250        |
| 15.1.1    | What is Blockchain? . . . . .                                 | 250        |
| 15.1.2    | Types of Blockchain . . . . .                                 | 253        |
| 15.1.3    | Blockchain in practice . . . . .                              | 255        |
| 15.1.4    | Humanitarian use cases . . . . .                              | 256        |
| 15.2      | Data Protection Impact Assessments . . . . .                  | 258        |
| 15.3      | Data Protection by design and by default . . . . .            | 260        |
| 15.4      | Data Controller/Data Processor relationship . . . . .         | 261        |
| 15.5      | Basic data protection principles . . . . .                    | 263        |
| 15.5.1    | Data minimization . . . . .                                   | 263        |
| 15.5.2    | Data retention . . . . .                                      | 264        |

|                                     |                                                                              |            |
|-------------------------------------|------------------------------------------------------------------------------|------------|
| 15.5.3                              | Proportionality . . . . .                                                    | 264        |
| 15.5.4                              | Data security . . . . .                                                      | 264        |
| 15.6                                | Rights of Data Subjects . . . . .                                            | 265        |
| 15.6.1                              | Right of access . . . . .                                                    | 266        |
| 15.6.2                              | Right to rectification . . . . .                                             | 266        |
| 15.6.3                              | Right to erasure . . . . .                                                   | 267        |
| 15.6.4                              | Restrictions of Data Subjects' rights . . . . .                              | 267        |
| 15.7                                | International Data Sharing . . . . .                                         | 268        |
| 15.8                                | Annex: Decision-making framework for Blockchain in Humanitarian Action . . . | 269        |
| <b>16</b>                           | <b>CONNECTIVITY AS AID . . . . .</b>                                         | <b>275</b> |
| <i>Aaron Martin and John Warnes</i> |                                                                              |            |
| 16.1                                | Introduction . . . . .                                                       | 276        |
| 16.1.1                              | Overview of connectivity as aid interventions . . . . .                      | 277        |
| 16.1.2                              | Operational context . . . . .                                                | 278        |
| 16.1.3                              | Multiple stakeholders and partnerships . . . . .                             | 279        |
| 16.2                                | Data Protection Impact Assessments . . . . .                                 | 281        |
| 16.3                                | Data Controller/Data Processor relationship . . . . .                        | 282        |
| 16.4                                | Basic data protection principles . . . . .                                   | 283        |
| 16.4.1                              | Legal bases for Personal Data Processing . . . . .                           | 283        |
| 16.4.2                              | Data security . . . . .                                                      | 284        |
| 16.4.3                              | Data retention . . . . .                                                     | 286        |
| 16.4.4                              | Information . . . . .                                                        | 286        |
| 16.5                                | International Data Sharing . . . . .                                         | 287        |
| <b>17</b>                           | <b>ARTIFICIAL INTELLIGENCE . . . . .</b>                                     | <b>289</b> |
| <i>Alessandro Mantelero</i>         |                                                                              |            |
| 17.1                                | Introduction . . . . .                                                       | 290        |
| 17.1.1                              | What Artificial Intelligence is and how it works . . . . .                   | 290        |
| 17.1.2                              | Artificial Intelligence in the humanitarian sector . . . . .                 | 294        |
| 17.1.3                              | Challenges and risks of using Artificial Intelligence . . . . .              | 299        |
| 17.2                                | Application of basic data protection principles . . . . .                    | 301        |
| 17.2.1                              | Legal bases for Personal Data Processing . . . . .                           | 302        |
| 17.2.2                              | Purpose limitation and Further Processing . . . . .                          | 305        |
| 17.2.3                              | Fair and lawful Processing . . . . .                                         | 308        |
| 17.2.4                              | Transparency . . . . .                                                       | 311        |
| 17.2.5                              | Data minimization . . . . .                                                  | 312        |
| 17.2.6                              | Data retention . . . . .                                                     | 314        |
| 17.2.7                              | Data security . . . . .                                                      | 315        |
| 17.3                                | Rights of Data Subjects . . . . .                                            | 316        |
| 17.3.1                              | Rights related to automated decision making . . . . .                        | 316        |



|                                                                                 |                |
|---------------------------------------------------------------------------------|----------------|
| CONTENTS                                                                        | xiii           |
| 17.4 Data Controller/Data Processor relationship . . . . .                      | 319            |
| 17.4.1 Accountability . . . . .                                                 | 319            |
| 17.4.2 Liability . . . . .                                                      | 320            |
| 17.5 International Data Sharing . . . . .                                       | 321            |
| 17.6 Data Protection Impact Assessment and Human Rights Impact Assessment . . . | 322            |
| 17.6.1 Human Rights Impact Assessment for Artificial Intelligence . . . . .     | 324            |
| 17.6.2 Human Rights Impact Assessment: phases and procedure . . . . .           | 325            |
| 17.7 Data Protection by design and by default . . . . .                         | 329            |
| 17.8 Ethical issues and challenges . . . . .                                    | 329            |
| <br><b>APPENDIX 1: TEMPLATE FOR A DPIA REPORT . . . . .</b>                     | <br><b>333</b> |
| <br><b>APPENDIX 2: WORKSHOP PARTICIPANTS . . . . .</b>                          | <br><b>339</b> |
| <br><b>INDEX . . . . .</b>                                                      | <br><b>343</b> |