

# Table of Contents

<i>Table of Cases</i>	xiii
<i>Table of Legislation</i>	xvii
<i>List of Abbreviations</i>	xix

1	Introduction	1
1.1	The lack of individual control in the data-driven economy	1
1.2	The individual in the data-driven (big-data) economy	3
1.2.1	Compromised privacy	3
1.2.2	Lack of transparency	5
1.2.3	Limited choice and autonomy	6
1.2.4	Discrimination	7
1.2.5	Power and control asymmetries	8
1.3	The need for enhanced data subject control and rights—regulatory response and the motivation for this book	9
1.4	A cautionary remark regarding scope	11
1.5	Introducing the main concepts	13
1.6	Structure	14
2	Safeguarding Individuals in the Data-driven Economy—EU Data Protection Framework in a Nutshell	16
2.1	Introduction	16
2.2	EU primary law	17
2.2.1	Introduction	17
2.2.2	The protection of an individual and her data in the EU system of fundamental rights	19
2.2.2.1	The ECHR system of protection of personal data and private life	19
2.2.2.1.1	The right to private life under Article 8 of the ECHR	19
2.2.2.1.2	Protection of personal data under Article 8 of the ECHR	21
2.2.2.2	Privacy and data protection as part of the EU framework of fundamental rights	22
2.2.2.2.1	The right to private life and protection of privacy of personal data under Article 7 of the EU Charter	23
2.2.2.2.2	The right to data protection in Article 8 of the EU Charter	23
2.2.2.2.2.1	The reasons to codify data protection as a human right	24
2.2.2.2.2.2	Differences between the data protection right and the right to privacy	26

2.3	EU secondary law	28
2.3.1	Introduction	28
2.3.2	Data protection law	28
2.3.2.1	General data protection	29
2.3.2.1.1	Personal data at the heart of data protection law	29
2.3.2.1.2	Protection-oriented duties of commercial data users	32
2.3.2.1.2.1	Definitions of data users	32
2.3.2.1.2.2	Personal data protection principles for personal data users	33
2.3.2.1.3	Control-enhancing rights of data subjects	37
2.3.2.1.3.1	Definition of data subjects	37
2.3.2.1.3.2	Data subject rights	37
2.3.2.2	Protection of privacy in public communication networks (ePrivacy)	38
2.3.3	Cybersecurity provisions	40
2.3.4	Competition law	42
2.3.5	Consumer protection law	45
2.4	Conclusions	47
3	Control as a Central Notion in the Discussion on Data Subject Rights	48
3.1	Introduction	48
3.2	Individual control over data and fundamental rights	49
3.2.1	Control over personal data and the right to informational self-determination	50
3.2.2	Control over personal data and the right to privacy	52
3.2.3	Control over personal data and the right to data protection	53
3.2.4	Control over personal data and the right to property	54
3.3	Control and EU data protection law	57
3.3.1	Policy vision for individual control in the data-driven economy	57
3.3.2	Reflections of control in the GDPR	59
3.3.3	Clustering control rights in the GDPR	60
3.4	Practical challenges	62
3.5	Conclusions	63
4	The Right to Information	64
4.1	Introduction	64
4.2	The link to fundamental values	65
4.3	Regulatory framework under the GDPR	66
4.3.1	The content of the communicated information	66
4.3.1.1	The information catalogue	66
4.3.1.1.1	Information about legal bases	69
4.3.1.1.2	Information about the length of the storage period	70
4.3.1.1.3	Information about third parties and recipients of data	71

4.3.1.1.4	Information about new (other) purposes of data processing	73
4.3.1.1.5	Information about the sources of data	75
4.3.1.2	The right to explanation	76
4.3.1.2.1	Information about automated decision-making in Articles 13 and 14	76
4.3.2	The quality of communication	80
4.3.3	The form of communicating information provisions	84
4.3.3.1	Privacy policies and/or notices	84
4.3.3.1.1	Icons and other visualisations	86
4.3.3.1.2	Standardised privacy policies	89
4.3.3.1.3	Information incorporated in standard terms and conditions	90
4.3.4	Timing	91
4.3.4.1	When in time?	91
4.3.4.2	How often in time?	93
4.3.5	Restrictions	93
4.4	The right to information in the electronic communication sector	96
4.4.1	Privacy of electronic communication	96
4.4.2	Informing about storing/accessing information in the terminal equipment of a subscriber	97
4.4.3	Informing users about collecting the information emitted by terminal equipment (such as geolocation information)	100
4.5	Conclusions and a short commentary through the lens of the data-driven economy	101
5	The Right of Access under EU Data Protection Law	104
5.1	Introduction	104
5.2	The right of access under the GDPR	106
5.3	The interface to submit requests and provide a copy of personal data	108
5.4	Regulatory boundaries to the right of access	111
5.4.1	Verification of identity	111
5.4.1.1	Timeline	112
5.4.1.2	Limitations of the right to access	113
5.4.1.3	Cost, frequency, and scope of data access requests	113
5.4.1.4	Conflict of rights	115
5.4.1.4.1	Conflict with the data controller's rights	116
5.4.1.4.2	Conflict with the right of other data subjects	118
5.4.1.4.3	Further exemptions	119
5.5	Challenges to the application of the right of access in the data-driven economy	120
5.5.1	The right of access on a continuum between personal and anonymised data	120
5.5.2	Accessing shared data and coupled databases	122
5.5.3	Access to information on automated decision-making	123
5.6	Conclusions and a short commentary through the lens of the data-driven economy	126

<b>6 The Right to Be Forgotten</b>	<b>129</b>
6.1 Introduction	129
6.2 Values underpinning the RTBF	130
6.3 Towards the GDPR's version of the RTBF	131
6.3.1 The right to oblivion in criminal law	132
6.3.2 The RTBF under the Data Protection Directive	132
6.3.3 The CJEU paving the way towards the GDPR in line with the 2012 proposal	133
6.3.3.1 Google Spain	134
6.3.3.2 Manni	139
6.4 The RTBF under the GDPR	141
6.4.1 The grounds to apply Article 17	141
6.4.1.1 'processing is no longer necessary in relation to the purposes for which it was collected'	141
6.4.1.2 'the data subject withdraws consent ... and where there is no other legal ground for the processing'	142
6.4.1.3 'the data subject objects to the processing'	143
6.4.1.4 'personal data was collected in relation to the offer of information society services directly to a child'	144
6.4.1.5 'erased for compliance with a legal obligation' or because 'the personal data was unlawfully processed'	145
6.4.2 Exceptions to the right to erasure	145
6.4.2.1 'processing is necessary for exercising the right of freedom of speech and information'	146
6.4.2.2 'processing is necessary for compliance with a legal obligation ... or for the performance of a task carried out in the public interest or in the exercise of official authority'	146
6.4.2.3 Other reasons	147
6.4.3 The meaning of 'informing third parties'	148
6.5 Options to operationalise the RTBF beyond the GDPR	150
6.5.1 My Account by Google and Privacy Basics by Facebook	151
6.5.1.1 Deletion by default	152
6.5.1.2 Expiration dates	153
6.5.1.3 Down-ranking	154
6.5.1.4 Deletion in the AI world	154
6.5.1.4.1 Unlearning of algorithms	154
6.5.1.4.2 Obfuscation	155
6.6 Conclusions and a short commentary through the lens of the data-driven economy	156
<b>7 Data Portability as a Data Subject Right</b>	<b>159</b>
7.1 Introduction	159
7.2 How and when the idea of data portability emerged	160
7.2.1 Commercial initiatives	160
7.2.2 Regulatory initiatives	162

7.3	Personal data portability under the GDPR	163
7.3.1	Three components of the right	164
7.3.1.1	‘The ... right to receive the personal data ... in a structured, commonly used and machine-readable format’	164
7.3.1.2	‘the right to transmit those data to another controller without hindrance’	165
7.3.1.3	‘the right to have the personal data transmitted directly from one controller to another, where technically feasible’	166
7.3.2	The restrictive definition of the right to data portability	167
7.3.2.1	‘data provided’	167
7.3.2.2	‘concerns a data subject’	168
7.3.2.3	‘The processing is based on consent ... or on a contract’	169
7.3.2.4	‘the processing is carried out by automated means’	169
7.3.2.5	‘The right should not apply to processing necessary for the performance of a task ... in the public interest or in the exercise of official authority’	170
7.3.2.6	‘That right shall not adversely affect the rights and freedoms of others’	170
7.4	Data portability versus other data subject rights	171
7.4.1	The right of access	171
7.4.2	The right to erasure (the RTBF)	172
7.4.3	The right to information	172
7.5	Data portability in other legal fields	173
7.5.1	Data portability as a competition law measure	174
7.5.2	Data portability as another aspect of the right to access industrial data	177
7.5.3	Personal data portability at the intersection between consumer and data protection	178
7.6	Unfolding the right to personal data portability as a control-affording entitlement	180
7.6.1	Data portability as a control-affording entitlement	180
7.6.1.1	Control over personal data transfers	181
7.6.1.2	Enabling control over (re)uses of data	182
7.6.1.3	Enabling control over multi-level data flows and complexity	184
7.6.1.4	Enabling free development of personality and equality	185
7.6.2	Data portability as a hindrance to data subject control	186
7.7	Conclusions	187
8	Data Subject Rights in Relation to Profiling	189
8.1	Introduction	189
8.2	Profiling as a building block of the data-driven value chain	190
8.2.1	The definition of profiling	191
8.2.2	Risks of profiling	194
8.2.2.1	Possible harms	194
8.2.2.2	Profiling with no human intervention—the real danger?	195

8.3	How the GDPR tackles profiling on the individual level	197
8.3.1	The GDPR's definition of profiling	197
8.3.2	The difficulties with asserting the legal basis for profiling	199
8.3.3	Individual rights in relation to profiling	201
8.3.3.1	The right to object	201
8.3.3.1.1	The nature of the right to object	201
8.3.3.1.2	The limits to the right to object	202
8.3.3.1.3	The right to object in the context of direct marketing	204
8.3.3.1.4	Technical implementation	205
8.3.3.2	The right not to be subject to solely automated decisions	205
8.3.3.2.1	The prohibition	205
8.3.3.2.2	The right to contest—technological due process?	209
8.4	Conclusions and a short commentary through the lens of the data-driven economy	212
9	Conclusions: Striving for Data Subject Control within and beyond Data Subject Rights	215
9.1	Introduction	215
9.1.1	The effectiveness assessment	216
9.1.1.1	Data subject control rights as a vehicle of lawfulness, transparency, and fairness	217
9.1.1.1.1	Lawfulness	217
9.1.1.1.2	Transparency	218
9.1.1.1.3	Fairness	220
9.1.1.2	Data subject rights as a vehicle of purpose limitation	222
9.1.1.3	Data subject rights as a vehicle of data minimisation and storage limitation	224
9.1.1.4	Data subject rights as a vehicle of accuracy, integrity, and confidentiality	225
9.1.1.5	Data subject rights as a vehicle of accountability	225
9.1.2	Concluding remarks	226
9.2	The way forward for data subject rights	227
9.2.1	Abandoning control rights	227
9.2.2	Alternatives to data subject rights	228
9.2.2.1	Turning to technological solutions	228
9.2.2.2	Legal solutions	230
9.2.2.2.1	Holistic approach within the GDPR	231
9.2.2.2.2	Holistic approach outside the GDPR	232
9.2.2.2.2.1	Consumer protection	232
9.2.2.2.2.2	Competition law	234
9.2.2.2.2.3	Regulation of AI	234
9.2.3	Concluding remarks	235
	<i>Bibliography</i>	237
	<i>Index</i>	265