

Contents

Foreword — V

Table of contents — IX

List of abbreviations — XXIX

Chapter 1

Introduction to data law — 1

- A. Introduction — 1
- B. The European digital strategy as a legal policy turning point in data law — 2
 - I. The European data strategy — 3
 - II. Evaluation — 6
- C. Data law – An attempt at systematisation — 7

Chapter 2

Data law — 10

- A. General part of Data law — 10
 - I. Data Act – Regulation (EU) 2023/2854 — 10
 - II. The Relationship of the Data Act to the General Data Protection Regulation and Trade Secrets Protection Law — 120
 - III. Legal framework for data governance under the Data Governance Act (DGA) – Regulation (EU) 2022/868 — 142
- B. Specific part of Data law — 196
 - I. Sector-specific data access regulations and the concept of European data spaces — 196
 - II. European Health Data Space (EHDS) — 199
 - III. Financial Data Access Regulation (FiDAR) — 208

Chapter 3

Regulation of data-based business models — 215

- A. Product-related regulation — 217
 - I. European cyber security law — 220
 - II. Regulation on Artificial Intelligence – Regulation (EU) 2024/1689 — 275
- B. Function-related regulation — 311
 - I. Platform-to-Business Regulation (P2BR) – Regulation (EU) 2019/1150 — 312
 - II. Digital Service Act (DSA) – Regulation (EU) 2022/2065 — 337
 - III. Digital Markets Act (DMA) – Regulation (EU) 2022/1925 — 399

Index — 434

Table of contents

Foreword — V
Contents — VII
List of abbreviations — XXIX

Chapter 1

Introduction to data law — 1

- A. Introduction — 1
- B. The European digital strategy as a legal policy turning point in data law — 2
 - I. The European data strategy — 3
 - 1. Pillar 1: A cross-sector governance framework for data access and use — 4
 - 2. Pillar 2: Investment in data infrastructures and European capacities — 5
 - 3. Pillar 3: Strengthening data competences and skills — 5
 - 4. Pillar 4: Creation of common European data spaces — 5
 - II. Evaluation — 6
- C. Data law – An attempt at systematisation — 7

Chapter 2

Data law — 10

- A. General part of Data law — 10
 - I. Data Act – Regulation (EU) 2023/2854 — 10
 - 1. Introduction — 12
 - 2. Scope and definitions, Art. 1–2 DA — 13
 - a) Territorial scope — 14
 - b) Temporal scope — 14
 - c) Material scope — 14
 - aa) Data, Art. 2 No. 1 DA — 15
 - (1) Primary data — 15
 - (2) Processed data — 16
 - (3) Metadata, Art. 2 No. 2 DA — 17
 - (4) Product data, Art. 2 No. 15 DA — 18
 - (5) Related service data, Art. 2 No. 16 DA — 18
 - (6) Readily available data, Art. 2 No. 17 DA — 18
 - (7) Data generated by virtual assistants, Art. 1(4) DA — 19
 - (8) Data and content not recorded — 19
 - bb) Connected product, Art. 2 No. 5 DA — 20
 - cc) Related service, Art. 2 No. 6 DA — 20
 - dd) Virtual assistants, Art. 2 No. 31 DA — 22
 - ee) Data processing service, Art. 2 No. 8 DA — 22

- d) Personal scope — **23**
 - aa) User, Art. 2 No. 12 DA — **23**
 - bb) Data holder, Art. 2 No. 13 DA — **24**
 - cc) Data recipients and third parties, Art. 2 No. 14 DA — **26**
 - dd) Manufacturer — **27**
 - ee) Contractual partner of the user — **27**
- 3. Rights and obligations of data holders, users and data recipients — **27**
 - a) Introduction — **27**
 - b) Obligations of the data holder when using the data — **28**
 - aa) Usage agreement requirement for readily available data (Art. 4(13) DA) — **29**
 - (1) Buy-out contracts — **30**
 - (2) Statement — **30**
 - bb) No authorisation for deletion of the data by the data holder — **31**
 - cc) Technical protective measures, Art. 11 DA — **32**
 - c) Use of the data by users — **33**
 - aa) Data access *by design*, Art. 3(1) DA — **34**
 - (1) Legal consequences of a breach of duty — **35**
 - (2) Direct access where relevant and technically feasible, Art. 3(1) DA — **36**
 - (3) Duty to inform, Art. 3(1), (2), (3) DA — **37**
 - bb) Data access claim of the user for readily available data, Art. 4 DA — **38**
 - (1) Provision modalities — **38**
 - (2) Concept of readily available data — **39**
 - (3) Separation of producer and data holder — **39**
 - (4) Checking the user status — **40**
 - (5) Handling of business secrets, Art. 4(6)–(9) DA — **41**
 - (a) Definition of trade secret — **42**
 - (b) Burden of proof of the trade secret holder, Art. 4(6) DA — **42**
 - (c) Disclosure under technical and organisational measures, Art. 4 DA — **43**
 - cc) Prohibition of data misuse, Art. 4(10) DA — **44**
 - dd) Obligation to use devices or services in good faith, Art. 4(11) DA — **44**
 - d) Use by and provision of data to third parties — **45**
 - aa) Provision of data only at the request of the user, Art. 8(4) DA — **45**
 - bb) Provision of readily available data to third parties at the request of the user, Art. 5(1) DA — **45**
 - (1) Modalities of provision, Art. 8–13 DA — **46**
 - (a) Agreement of appropriate conditions, Art. 8(1) DA — **46**

	(b) Prohibition of discrimination, Art. 8(3) DA —	48
	(c) Consideration for the provision of data, Art. 9 DA —	48
	(d) Handling of business secrets (Art. 8(6) DA) —	49
	(2) Obligations of third parties who receive data at the user's request (Art. 6 DA) —	49
	(a) Individual obligations of the third party —	49
	(b) Re-disclosure of data to other third parties, Art. 6(2)(c) DA —	50
	(3) Exclusion for gatekeepers (Art. 5(3) DA) —	51
	cc) Disclosure of data to third parties by the user himself —	53
	e) Dispute resolution by dispute resolution bodies (Art. 10 DA) —	54
4.	Unfair contract terms unilaterally imposed on another company, Art. 13 DA —	56
	a) Background —	56
	b) Scope of the clause control: B2B contracts —	57
	aa) Contractual clauses relating to data access and use or liability and remedies for breach or termination of data-related obligations —	58
	bb) Imposed unilaterally —	59
	(1) Requirement of a negotiation attempt? —	59
	(2) Statement —	60
	cc) Relationship to the control of general terms and conditions under national law, Art. 1(9) DA —	61
	c) Abuse control —	62
	aa) "Blacklist" (Art. 13(4) (a)–(c)) —	63
	bb) "Grey list" (Art. 13(5)(a)–(g) DA) —	64
	cc) General clause (Art. 13(3) DA) —	64
	d) Legal consequences and enforcement —	65
	e) Practical recommendations —	67
5.	Provision of data to public authorities, the Commission, the European Central Bank and Union bodies on grounds of exceptional necessity, Art. 14–22 DA —	68
	a) Area —	68
	aa) Exceptional necessity of data use, Art. 15 DA —	68
	(1) Management of a public emergency, Art. 15(1)(a) DA —	68
	(2) Enabling the fulfilment of tasks, Art. 15(1)(b) DA —	69
	(3) Exemption for micro and small enterprises and exemption from the obligation to provide evidence, Art. 15(2), (3) DA —	70
	bb) Authorised applicants, Art. 14 DA —	70
	cc) Obligated parties —	71
	dd) Further requirements —	71
	ee) Exceptions, Art. 16 DA —	71

- b) Requirement for data provision requests and prohibition of further use, Art. 17(1)–(3) DA — **72**
 - c) Fulfilment of data requests, Art. 18 DA — **72**
 - d) Obligations in handling the data received, Art. 19 DA — **73**
 - e) Compensation in the event of exceptional necessity, Art. 20 DA — **74**
- 6. Switching between data processing services, Art. 23–31 DA — **75**
 - a) Preliminary considerations and background to the regulation of data processing services — **75**
 - b) Data processing service, Art. 2 No. 8 DA — **77**
 - aa) Scope of the area in question — **77**
 - bb) Further characteristics of the data processing service — **78**
 - c) The switching process — **80**
 - aa) Change, Art. 2 No. 34 DA — **81**
 - bb) Customer, Art. 2 No. 30 DA — **81**
 - cc) ICT infrastructure on own premises, Art. 2 No. 33 DA — **81**
 - dd) Same type of service, Art. 2 No. 9 DA — **82**
 - ee) Functional equivalence, Art. 2 No. 37 DA — **82**
 - ff) Distinctions from the switching process — **83**
 - gg) Object of the bill of exchange — **83**
 - (1) Exportable data, Art. 2 No. 38 DA — **84**
 - (2) Digital assets, Art. 2 No. 32 DA — **84**
 - d) Barriers to exchange, Art. 23 DA — **84**
 - e) Obligations for data processing services, Art. 23–31 DA — **85**
 - aa) Prohibition of imposition and obligation to remove, Art. 23 p. 2 DA — **86**
 - bb) Contractual clauses for the bill of exchange, Art. 25 DA — **86**
 - (1) Clauses on the decision to switch, Art. 25(3) DA — **87**
 - (2) Minimum content obligations, Art. 25(2) DA — **87**
 - (a) Change request and transition period, Art. 25(2)(a) DA — **88**
 - (b) Exit strategy, Art. 25(2)(b) DA — **89**
 - (c) Termination of contract and notification of cancellation, Art. 25(2)(c) DA — **89**
 - (d) Maximum notice period, Art. 25(2)(d) DA — **89**
 - (e) Listing of data categories, digital assets and restriction on business secrets, Art. 25 (2)(e) and (f) DA — **90**
 - (f) Minimum period for data retrieval of 30 days, Art. 25 (2)(g) DA — **90**
 - (g) Deletion of the data, Art. 25(2)(h) DA — **90**
 - (h) Exchange fees, Art. 25(2)(i) DA — **90**
 - (3) Extension of the transitional period, Art. 25(4) and (5) DA — **90**

- cc) Duty to inform, Art. 26 DA — **91**
- dd) Cooperation in good faith, Art. 27 DA — **92**
- ee) Transparency obligations, Art. 28 DA — **92**
- f) Gradual abolition of exchange fees, Art. 29 DA — **93**
 - aa) Exchange fees (Art. 2 No. 36 DA) and data extraction fees (Art. 2 No. 35 DA) — **93**
 - bb) Duty to provide information on exchange fees, Art. 29(4)–(6) DA — **95**
- g) Technical aspects of the bill of exchange, Art. 30 DA — **95**
- h) Exceptions, Art. 31 DA — **97**
 - aa) Individual solutions, Art. 31(1) DA — **97**
 - bb) Data processing services for testing and evaluation purposes, Art. 31(2) DA — **97**
 - cc) Obligation of the provider to inform about non-applicable obligations, Art. 31(3) DA — **98**
- i) Sanctions and enforcement — **98**
- 7. Unlawful government access to and unlawful government transfer of non-personal data in an international context, Art. 32 DA — **99**
 - a) Background and area — **99**
 - b) Duty to prevent international transfer and access by government organisations, Art. 31(1) DA — **100**
 - c) Exceptions, Art. 31(2), (3) DA — **100**
- 8. Interoperability, Art. 33–36 DA — **101**
 - a) Overview and systematics — **101**
 - b) Interoperability of data rooms, Art. 33 DA — **102**
 - aa) Participants in data rooms (1) — **102**
 - bb) Essential requirements (1) — **103**
 - cc) Concretisation through delegated acts (2) — **103**
 - dd) Presumption of conformity, harmonised standards, common specifications (3)–(11) — **103**
 - c) Interoperability for the parallel use of data processing services, Art. 34 DA — **104**
 - d) Interoperability of data processing services, Art. 35 DA — **105**
 - aa) Regulatory objectives and minimum requirements (1) and (2) — **105**
 - bb) Creation of standards (3)–(9) — **106**
 - e) Smart Contracts, Art. 36 DA — **106**
 - aa) Obligated party, application, data transfer agreement — **107**
 - bb) Essential requirements (1) — **108**
 - cc) Conformity assessment (2)–(3) — **108**
 - dd) Presumption of conformity (4)–(11) — **109**

9.	Application and enforcement, Art. 37–42 DA —	109
a)	Competent authorities and data coordinators, Art. 37 DA —	109
aa)	Competent authorities, Art. 37(1) DA —	109
bb)	Tasks of the competent authorities, Art. 37(5), (8), (9), (14) DA —	110
cc)	Data Coordinator, Art. 37(2) DA —	110
dd)	Responsibilities for legal entities, Art. 37(10)–(13) DA —	111
ee)	Administrative cooperation between Member State authorities, Art. 37(15), (16) DA —	112
b)	Right to lodge a complaint, Art. 38 DA —	112
aa)	Possibility of private enforcement? —	112
bb)	Statement —	113
c)	Right to an effective judicial remedy, Art. 39 DA —	113
d)	Sanctions, Art. 40 DA —	114
e)	Model contract clauses and standard contract clauses, Art. 41 DA —	115
f)	Role of the European Data Innovation Board (EDIB) Art. 42 DA —	116
10.	Databases containing certain data, Art. 43 DA —	116
11.	Final provisions, Art. 44–50 DA —	117
12.	Summary and implications for practice —	118
II.	The Relationship of the Data Act to the General Data Protection Regulation and Trade Secrets Protection Law —	120
1.	Introduction —	121
2.	Data Act and GDPR —	122
a)	Conflict between Data Act and GDPR for mixed data sets —	122
b)	Conflict of laws, Art. 1(5) DA —	123
c)	Personal roles —	124
aa)	Key players of the GDPR —	124
bb)	Key players in the DA —	124
cc)	Tension between the personal roles —	125
d)	Access claims under Art. 4, 5 DA —	125
aa)	Consent, Art. 6(1)(a) GDPR —	126
(1)	Voluntariness —	126
(2)	Practical relevance —	127
bb)	Fulfilment of a contract, Art. 6(1)(b) GDPR —	127
cc)	Fulfilment of a legal obligation, Art. 6(1)(c) GDPR —	128
dd)	Legitimate interest, Art. 6(1)(f) GDPR —	129
ee)	Summary —	130
e)	Special categories of personal data pursuant to Art. 9 GDPR —	131
f)	Data access rights (Art. 4, 5 GDPR) and data portability (Art. 20 GDPR) —	132
g)	Legal basis for the processing of personal data in the context of data access claims pursuant to Art. 4, 5 DA and B2G data access pursuant to Art. 14 et seq. DA —	132

h)	Risk of fines —	133
i)	Conclusion —	134
3.	Data Act and trade secret protection law —	134
a)	Directive (EU) 2016/943 —	135
aa)	Area —	135
bb)	Lawful and unlawful use, Art. 3, 4, 5 Directive (EU) 2016/943 —	137
b)	Relationship between the Directive (EU) 2016/943 and the Data Act —	138
aa)	Requirements for the provision of trade secrets, Art. 4 DA —	138
(1)	Right of refusal pursuant to Art. 4(7) DA —	139
(2)	Right of refusal pursuant to Art. 4(8) DA —	140
bb)	Disclosure of trade secrets to third parties, Art. 5 DA —	140
(1)	Restriction of data access by third parties pursuant to Art. 5(9) DA —	140
(2)	Rights of refusal pursuant to Art. 5(10) and (11) DA —	141
cc)	Summary —	141
4.	Summary and implications for practice —	142
III.	Legal framework for data governance under the Data Governance Act (DGA) – Regulation (EU) 2022/868 —	142
1.	Introduction —	144
a)	Problem analysis of the status quo —	144
b)	Importance and function of data governance —	145
c)	Principles and systematics of the DGA —	147
d)	Demarcation of the DGA from the GDPR —	148
aa)	Legal requirements for demarcation —	149
bb)	Criticism —	150
2.	Data held by public sector bodies, Art. 3–9 DGA —	151
a)	Sense and purpose of the regulations —	151
b)	Addressees of the provisions of the second chapter —	152
c)	No obligation of public sector bodies to disclose, Art. 1(2) DGA —	153
d)	Objectively recorded data and actions, Art. 3(1) DGA —	154
aa)	Re-use of the data —	154
bb)	Data held by public sector bodies —	155
cc)	Specially protected data —	155
(1)	First data group: Commercial confidentiality to Art. 3(1)(a) DGA —	156
(2)	Second data group: Statistical confidentiality pursuant to Art. 3(1)(b) DGA —	156
(3)	Third data group: Intellectual property pursuant to Art. 3(1)(c) DGA —	156
(4)	Fourth data group: Protection of personal data pursuant to Art. 3(1)(d) DGA —	157

- e) Exclusion of certain types of data in Art. 3(2)(d), (e) DGA — **157**
- f) Prohibition of exclusive arrangements, Art. 4 DGA — **158**
- g) Conditions for re-use, Art. 5 DGA — **159**
 - aa) Protective measures for personal data — **160**
 - bb) Protective measures for non-personal data — **162**
- h) Fees for re-use, Art. 6 DGA — **163**
- i) Management of re-utilisation procedures, Art. 7, 8, 9 DGA — **163**
- j) Criticism — **164**
- 3. Data intermediaries and data intermediation services — **165**
 - a) The term “data intermediation service”, Art. 2 No. 11 DGA — **165**
 - aa) Initiation of business relationships — **166**
 - bb) Practices that constitute data intermediation services — **167**
 - cc) No data intermediation services — **169**
 - dd) Summary — **171**
 - b) Obligations of data intermediation services — **171**
 - aa) Data intermediation service within the meaning of Art. 10 DGA — **172**
 - (1) Intermediary services between data holders and potential data users, Art. 10(a) DGA — **172**
 - (2) Intermediary services between data subjects or natural persons and data users, Art. 10(b) DGA — **172**
 - (3) Services of data cooperatives, Art. 10(c) DGA — **173**
 - bb) Registration according to Art. 11 DGA — **173**
 - cc) Catalogue of obligations under Art. 12 DGA — **175**
 - c) Law enforcement — **179**
 - d) Criticism — **181**
- 4. Data altruism, Art. 16–25 DGA — **183**
 - a) Concept, function and principle of data altruism — **183**
 - b) National arrangements for data altruism, Art. 16 DGA — **184**
 - c) Recognised data altruism organisations, Art. 17–19 DGA — **185**
 - d) Transparency, protection and procedural requirements of data altruistic organisations, Art. 20–22, 25 DGA — **186**
 - e) Law enforcement: Competent authorities and monitoring practice, Art. 23, 24 DGA — **189**
- 5. Other regulations — **189**
 - a) The European Data Innovation Board, Art. 29 et seq. et DGA — **189**
 - aa) Organisation of the Data Innovation Board — **189**
 - bb) Tasks and responsibilities of the Board — **190**
 - b) International access and transfer, Art. 31 DGA — **190**
 - aa) The principle according to Art. 31(1) DGA — **191**
 - bb) Exceptions to the principle according to Art. 31(1) DGA — **191**
 - (1) International agreement pursuant to Art. 31(2) DGA — **191**

- (2) Comparable rule of law standards pursuant to Art. 31(3) DGA — **192**
- 6. Supervision, enforcement and sanctions — **192**
- 7. Summary and practical implications — **194**
- B. Specific part of Data law — **196**
 - I. Sector-specific data access regulations and the concept of European data spaces — **196**
 - II. European Health Data Space (EHDS) — **199**
 - 1. Introduction — **200**
 - a) Legislative procedure — **200**
 - b) Goals — **201**
 - c) Structure and systematics of the EHDS — **202**
 - 2. Rights and obligations of the parties involved — **203**
 - a) Primary use of electronic health data — **203**
 - b) Secondary use of electronic health data — **205**
 - 3. Supervision, enforcement and sanctions — **206**
 - 4. Summary and practical implications — **207**
 - III. Financial Data Access Regulation (FiDAR) — **208**
 - 1. Introduction — **209**
 - 2. Scope, Art. 2 FiDAR-D — **210**
 - 3. Data access claims, Art. 4–7 FiDAR-D — **211**
 - a) Access by the customer, Art. 4 FiDAR-D — **211**
 - b) Access by a data user, Art. 5(1) FiDAR-D — **212**
 - c) Authorisation dashboard, Art. 8(1) FiDAR-D — **212**
 - 4. Data sharing systems, Art. 9–11 FiDAR-D — **213**
 - 5. Summary and practical implications — **214**

Chapter 3

Regulation of data-based business models — 215

- A. Product-related regulation — **217**
 - I. European cyber security law — **220**
 - 1. Network and Information Security Directive (NIS) – Directive (EU) 2022/2555 — **220**
 - a) Introduction — **220**
 - b) Scope, Art. 2 Directive (EU) 2022/2555 — **221**
 - aa) Establishment, Art. 6 No. 38 Directive (EU) 2022/2555 — **221**
 - bb) Facilities covered regardless of their size, Art. 2(2) Directive (EU) 2022/2555 — **221**
 - cc) Essential and important facilities, Art. 3(1), (2) Directive (EU) 2022/2555 — **222**

c)	Obligations of covered entities, Art. 20 et seq. Directive (EU) 2022/2555 —	222
aa)	Risk management measures in the area of cybersecurity, Art. 21 Directive (EU) 2022/2555 —	222
bb)	Reporting obligations, Art. 23 Directive (EU) 2022/2555 —	223
cc)	Utilisation of the European schemes for cybersecurity certification, Art. 24 Directive (EU) 2022/2555 —	225
d)	Supervision, enforcement and sanctions, Art. 31–37 Directive (EU) 2022/2555 —	225
e)	Summary and practical implications —	226
2.	Cybersecurity Act (CSA) – Regulation (EU) 2019/881 (overview) —	228
3.	Cyber Resilience Act (CRA) – Regulation (EU) 2024/2847 —	229
a)	Introduction —	230
b)	Interaction with other legal acts —	231
aa)	NIS 2-RL —	232
bb)	CSA —	232
cc)	GDPR —	232
dd)	Product Safety Regulation —	232
ee)	Product Liability Directive —	233
ff)	Regulation on the European Digital Identity (EUDI) —	233
gg)	AIA —	233
c)	Scope and definition —	234
aa)	Material scope: Products with digital elements, Art. 2(1) CRA —	234
bb)	Personal scope —	235
cc)	Temporal scope, Art. 69(2) CRA —	236
dd)	Area exceptions —	236
(1)	Cloud provider —	236
(2)	Exemptions for certain product groups, Art. 2(2)–(7), Art. 4(2)–(3) CRA —	237
d)	General provisions of the CRA —	238
aa)	Categorisation of the cyber security risk —	238
(1)	Level 1: Products with digital elements, Art. 6 CRA —	238
(2)	Level 2: Important products with digital elements, Art. 7(1) in conjunction with Annex III CRA —	239
(3)	Level 3: Critical products with digital elements, Art. 8 in conjunction with Annex IV CRA —	240
bb)	The different conformity assessment procedures —	240
(1)	The effect of the presumption of conformity, Art. 27 CRA —	241
(2)	The conformity assessment procedures in detail, Art. 32(1)–(4) CRA —	241
e)	Rights and obligations of economic operators, Art. 13–26 CRA —	243
aa)	General obligations —	243

- bb) Obligations of manufacturers of products with digital elements — **243**
- cc) Obligations regarding the placing on the market, Art. 13 CRA — **243**
 - (1) Product requirements, Annex I Part 1 CRA — **244**
 - (2) Obligations after placing on the market, Art. 13(8)–(20) in conjunction with Annex I Part II CRA — **245**
 - (3) Reporting obligations, Art. 14 CRA — **246**
 - (a) Notification of an actively exploited vulnerability, Art. 14(1) CRA — **246**
 - (b) Notification of a serious incident, Art. 14(3) CRA — **247**
 - (c) Addressee of the notification, Art. 14(1), (3) CRA — **248**
 - (d) Single reporting platform, Art. 16(1) CRA — **249**
- dd) Obligations of importers and distributors of products with digital elements, Art. 19–22 CRA — **250**
 - (1) Obligations of importers — **251**
 - (2) Obligations of dealers — **251**
 - (3) Common obligations — **252**
- ee) Special case: open source software stewards, Art. 24 CRA — **252**
 - (1) Concept and special features of the scope — **253**
 - (2) Voluntary control — **253**
 - (3) Obligations and exceptions for stewards — **254**
- f) Market surveillance, enforcement and sanctions — **254**
 - aa) Market surveillance and enforcement, Art. 52–60 CRA — **255**
 - bb) Sanctions, Art. 64 CRA — **255**
 - (1) Breaches of cybersecurity requirements in accordance with Annex I and Art. 13, 14, Art. 64(2) CRA — **256**
 - (2) Violations of Art. 18–53, Art. 63(3) CRA — **256**
 - (3) Incomplete, misleading or false information provided to the notified body or market surveillance authority, Art. 64(4) CRA — **256**
 - (4) Exception for SMEs and administrators of open source software, Art. 64(10) CRA — **256**
- g) Summary and practical implications — **256**
- 4. Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554 — **260**
 - a) Preliminary considerations — **260**
 - aa) Introduction and background to the regulation — **260**
 - bb) Relationship to other European cybersecurity law — **262**
 - b) Scope, Art. 2 DORA — **262**

- c) Obligations for financial companies, Art. 5–35 DORA — **263**
 - aa) Obligations under the ICT risk management framework, Art. 5–14 DORA — **264**
 - (1) Organisational duties of the management body, Art. 5(2) DORA — **264**
 - (2) Duty of the management body to provide further training, Art. 5(4) DORA — **265**
 - (3) Obligation to update for ICT systems, protocols and tools, Art. 7 DORA — **266**
 - (4) Identification of ICT risks, Art. 8 DORA — **266**
 - (5) Protection and prevention of incidents, Art. 9 DORA — **266**
 - (6) Recognition mechanisms, Art. 10 DORA — **267**
 - (7) Response to incidents, Art. 11 DORA — **267**
 - (8) Guidelines and procedures for backup, recovery and restoration, Art. 12 DORA — **267**
 - (9) Further development obligation, Art. 13 DORA — **268**
 - (10) Communication plans, Art. 14 DORA — **268**
 - bb) Simplified ICT risk management framework, Art. 16 DORA — **269**
 - cc) ICT third party risk management, Art. 28–30 DORA — **269**
- d) ICT-related incidents – handling and reporting, Art. 17–19 DORA — **270**
- e) Testing digital resilience through test programmes, Art. 24–27 DORA — **271**
 - aa) Basic testing obligation, Art. 24 DORA — **271**
 - bb) Threat-Led Penetration Tests, Art. 25–27 DORA — **271**
- f) Supervision, enforcement and sanctions, Art. 46 et seqq. DORA — **272**
 - aa) Supervision and enforcement, Art. 46, 47 DORA — **272**
 - bb) Sanctions, Art. 50–54 DORA — **273**
 - (1) Administrative sanctions, Art. 50 DORA — **273**
 - (2) Criminal sanctions, Art. 52 DORA — **273**
- g) Conclusion — **274**
 - aa) Summary — **274**
 - bb) Practical guide — **274**

II. Regulation on Artificial Intelligence – Regulation (EU) 2024/1689 — **275**

- 1. Introduction — **276**
 - a) Background to the regulation of artificial intelligence — **276**
 - b) Objectives and recitals — **277**
 - c) Demarcations — **277**
- 2. Scope and definitions — **278**
 - a) Material scope — **278**
 - aa) AI systems, Art. 3 No. 1 AIA — **278**
 - bb) AI models with general purpose, Art. 3 No. 63 AIA — **279**

- b) Personal scope — **280**
 - aa) Provider, Art. 3 No. 3 AIA — **281**
 - bb) Deployer, Art. 3 No. 4 AIA — **281**
 - c) Territorial scope — **281**
 - d) Area exceptions — **281**
- 3. Rights and obligations — **282**
 - a) AI literacy, Art. 4 AIA — **283**
 - b) Prohibited AI practices, Art. 5 AIA — **284**
 - c) High-risk AI systems, Art. 6–49 AIA — **285**
 - aa) Classification of AI systems as high-risk, Art. 6 AIA — **285**
 - (1) Classification in accordance with Art. 6(1) AIA (Annex I) — **286**
 - (2) Classification in accordance with Art. 6(2) AIA (Annex III) — **286**
 - (3) Exceptions, Art. 6(3) AIA — **286**
 - bb) Requirements for high-risk AI systems, Art. 8–15 AIA — **288**
 - cc) Obligations of providers and deployers of high-risk AI systems, Art. 16–22 AIA — **289**
 - (1) Obligations of providers of high-risk AI systems, Art. 16 AIA — **290**
 - (2) Quality management system, Art. 17 AIA — **290**
 - (3) Documentation keeping, Art. 18 AIA — **290**
 - (4) Automatically generated logs, corrective actions and duty to inform, Art. 19, 20 AIA — **290**
 - (5) Cooperation with the competent authorities and authorised representatives of providers, Art. 21, 22 AIA — **291**
 - dd) Obligations of importers of high-risk AI systems, Art. 23 AIA — **291**
 - ee) Obligations of distributors of high-risk AI systems, Art. 24 AIA — **291**
 - ff) Obligations of deployer of high-risk AI systems, Art. 26 AIA — **292**
 - (1) Purposeful input data, monitoring obligation and retention obligation for automatically generated logs, Art. 26(4)–(6) AIA — **293**
 - (2) Information obligations, Art. 26(7), (11) AIA — **293**
 - (3) Registration, data protection impact assessment and high-risk AI system for subsequent biometric identification, Art. 26(8), (9), (10) AIA — **293**
 - (4) Fundamental rights impact assessment, Art. 27 AIA — **294**
 - d) Transparency obligations for providers and deployers of certain AI systems, Art. 50 AIA — **294**
 - aa) AI systems with direct interaction with natural persons (Art. 50(1) AIA) — **295**
 - bb) AI systems for the generation of synthetic audio, image, video or text content (Art. 50(2) AIA) — **295**

cc)	Emotion recognition systems or systems for biometric categorisation (Art. 50(3) of the AIA) —	295
dd)	AI systems for the generation and manipulation of image, sound or video content, deepfakes and texts for public information (Art. 50(4) AIA) —	296
e)	AI models with a general purpose, Art. 51–56 AIA —	297
aa)	Classification, Art. 51 AIA —	297
bb)	Obligations for providers of general purpose AI models, Art. 53 AIA —	298
cc)	Obligations for providers of general purpose AI models with systemic risk, Art. 55 AIA —	299
dd)	Practical guidelines, Art. 56 AIA —	299
ee)	Standards, conformity assessment, certificates, registration, Art. 40–49 AIA —	300
4.	Notifying authorities and notified bodies, Art. 28–39 AIA —	301
5.	Governance —	302
a)	Office for Artificial Intelligence (AI Office), Art. 64 AIA —	302
b)	AI Board (AI Board), Art. 65, 66 AIA —	303
c)	Market surveillance authority, Art. 3 No. 26 AIA —	303
6.	Sanctions —	305
a)	Fines —	305
aa)	Violation of prohibited practices in the AI sector, Art. 99(3) AIA —	305
b)	Further liability risks —	305
c)	Legal remedies —	307
7.	Summary and implications for practice —	307
a)	General criticism of the regulatory concept —	307
b)	In detail —	308
aa)	Impending legal uncertainty and lack of clarity regarding the purpose of the law —	309
bb)	Diffuse regulatory purposes —	309
c)	Practical implications —	310
B.	Function-related regulation —	311
I.	Platform-to-Business Regulation (P2BR) – Regulation (EU) 2019/1150 —	312
1.	Introduction —	313
a)	Backgrounds —	313
b)	Goals —	314
c)	Differentiation from other legal acts of platform regulation —	315
2.	Scope, Art. 1(1), (2) P2BR —	315
a)	Personal scope —	315
aa)	The customer relationship —	315
bb)	The supplier-side relationship —	315

cc)	The customer-provider relationship —	316
b)	Material scope, Art. 2 P2BR —	317
aa)	Online intermediary services, Art. 2 No. 2 P2BR —	317
(1)	Definition —	317
(a)	Service of an information society, Art. 2 No. 1(a) P2BR —	317
(b)	Mediation of the initiation of transactions between business users and consumers —	318
(c)	Provision of brokerage by contractual basis, Art. 2 No. 2(c) P2BR —	319
(aa)	Effectiveness of the contract —	319
(bb)	Declaration on a durable medium, Art. 2 No. 13 P2BR —	319
(2)	Examples —	320
bb)	Online search engines, Art. 2 No. 5 P2BR —	320
cc)	Territorial scope, Art. 1(1) P2BR —	321
3.	Requirements for online brokerage services and online search engines —	322
a)	Online brokerage services —	322
aa)	GTC, Art. 3 P2BR —	322
(1)	Obligations to include general terms and conditions, Art. 3(1) P2BR —	323
(2)	Obligations in the event of changes to the GTC, Art. 3(2) P2BR —	324
(3)	Nullity of general terms and conditions, Art. 3(3) P2BR —	324
(4)	Competitions —	325
bb)	Restriction, suspension and termination, Art. 4 P2BR —	325
cc)	Rankings, Art. 5 P2BR —	326
(1)	Regulatory objective —	326
(2)	Specifications —	326
(3)	Delimitation to Art. 26, 27 DSA —	327
dd)	Differentiated treatment, Art. 7 P2BR —	327
(1)	Regulatory objective —	327
(2)	Specifications —	328
ee)	Special contractual provisions, Art. 8 P2BR —	328
ff)	Data access, Art. 9 P2BR —	329
(1)	Regulatory objective —	329
(2)	Requirements, Art. 9(2) P2BR —	330
gg)	Restriction on the possibility of introducing other conditions by other means Art. 10 P2BR —	330
hh)	Internal complaints management, Art. 11 P2BR —	331
(1)	Regulatory objective —	331

	(2) Specifications —	331
	(3) Demarcation —	332
	ii) Duty to mediate, Art. 12 P2BR —	332
b)	Online search engines —	333
	aa) Ranking, Art. 5 P2BR —	333
	bb) Differentiated treatment, Art. 7 P2BR —	333
4.	Enforcement and supervision —	334
a)	Civil liability —	334
	aa) Claims under national law, Art. 15 P2BR —	334
	bb) Filing a complaint, Art. 14 P2BR —	334
b)	Supervision, Art. 15 P2BR —	335
c)	Example Germany —	335
5.	Summary and implications for practice —	336
II.	Digital Service Act (DSA) – Regulation (EU) 2022/2065 —	337
1.	Introduction —	338
a)	Background and relationship to the E-Commerce Directive, Art. 2, 89 DSA —	338
b)	Legal policy considerations —	339
c)	Concrete goals —	341
d)	Basic structure —	342
2.	Area —	343
a)	Material-personal scope —	343
	aa) Intermediary services, Art. 3(g) DSA —	344
	bb) Individual intermediary services, Art. 3(g)(i)–(iii) DSA —	344
	(1) Pure transit, Art. 3(g)(i) DSA —	344
	(2) Caching service, Art. 3(g)(ii) DSA —	345
	(3) Hosting service, Art. 3(g)(iii) DSA —	346
	cc) Online search engine as intermediary services, Art. 3(j) DSA —	346
b)	Territorial scope (market place principle), Art. 2(1) DSA —	348
3.	(Due diligence) obligations and liability of providers of intermediary services, Art. 4–48 DSA —	350
a)	General liability concept, Art. 4–6 DSA —	350
	aa) Liability privileges as a cornerstone of platform regulation —	350
	bb) Subjective scope: Information society services —	351
	cc) Material scope: Information provided by users —	352
	dd) Obligations of the individual mediation services —	353
	(1) Pure transit, Art. 4 DSA —	353
	(2) Caching, Art. 5 DSA —	354
	(3) Hosting, Art. 6 DSA —	354
	ee) Good Samaritan privilege, Art. 7 DSA —	355
b)	No general obligation to monitor or actively investigate, Art. 8 DSA —	356

- c) Judicial and official orders, Art. 9–10 DSA — **357**
 - aa) Orders to take action against illegal content, Art. 9 DSA — **357**
 - bb) Requests for information, Art. 10 DSA — **357**
- d) Due diligence and transparency obligations for brokerage services — **357**
 - aa) Level 1: Regulations for providers of intermediary services, Art. 11–15 DSA — **358**
 - (1) Contact point for authorities and users and legal representatives, Art. 11–13 DSA — **358**
 - (2) GTC, Art. 14 DSA — **359**
 - (3) Transparency reporting obligations, Art. 15 DSA — **361**
 - bb) Level 2: Rules for hosting services, Art. 16–18 DSA — **361**
 - (1) Reporting and redress procedures Art. 16 DSA — **361**
 - (2) Justification, Art. 17 DSA — **363**
 - (3) Reporting of criminal offences, Art. 18 DSA — **363**
 - cc) Level 3: Additional provisions for online platforms, Art. 19–28 DSA — **364**
 - (1) Internal complaints management system, Art. 20 DSA — **364**
 - (2) Out-of-court dispute resolution, Art. 21 DSA — **365**
 - (3) “Trusted flagger”, Art. 22 DSA — **367**
 - (4) Measures and protection against misuse, Art. 23 DSA — **367**
 - (5) Transparency obligations, Art. 24, 27 DSA — **368**
 - (a) Transparency reporting obligation of online platform providers, Art. 24 DSA — **368**
 - (b) Transparency of recommendation systems, Art. 27 DSA — **368**
 - (6) Design and organisation of the online interface, Art. 25 DSA (*Dark Patterns*) — **368**
 - (7) Online advertising and recommendation system, Art. 26 DSA — **371**
 - (8) Transparency of recommendation systems, Art. 27 DSA — **372**
 - (9) Online protection of minors, Art. 28 DSA — **372**
 - (10) Further consumer protection provisions, Art. 30–32 DSA — **373**
 - dd) Stage 4: Regulations for very large platforms and very large search engines — **374**
 - (1) Scope, Art. 33 DSA — **375**
 - (2) Tightening of the catalogue of obligations applicable to online platforms — **376**
 - (3) Risk assessment, Art. 34 DSA — **377**
 - (4) Risk minimisation, Art. 35 DSA — **378**
 - (5) Rapid response mechanism and protocols, Art. 36, 48 DSA — **379**

	(6) Independent audit, Art. 37 DSA —	381
	(7) Data access and control, Art. 40 DSA —	383
	(8) Compliance department, Art. 41 DSA —	384
	(9) Supervisory fees, Art. 43 DSA —	385
4.	Supervision and enforcement, Art. 49–63 DSA —	386
a)	Supervision and enforcement by the Member States, Art. 49–55 DSA —	386
b)	Compensation Art. 54 DSA —	388
c)	Coordinated investigations and coherence mechanisms, Art. 57 DSA —	388
d)	European Digital Services Board, Art. 61–63 DSA —	389
e)	Enforcement of obligations of providers of very large online platforms and very large online search engines —	391
aa)	Supervisory responsibility, Art. 66 DSA —	391
bb)	Powers of the Commission —	392
cc)	Non-compliance and sanctions, Art. 73 ff DSA —	392
dd)	Overview of sanctions —	393
5.	Summary and implications for practice —	397
III.	Digital Markets Act (DMA) – Regulation (EU) 2022/1925 —	399
1.	Introduction —	400
a)	Economic background of the DMA —	400
b)	Objectives of the DMA —	402
c)	Relationship to European and national competition law —	403
d)	Relationship to the Digital Services Act —	404
2.	Material and territorial scope, Art. 1(2) DMA —	405
a)	Central platform services, Art. 2 No. 2 DMA —	405
b)	Appointment as gatekeeper, Art. 3 DMA —	406
aa)	Qualitative and quantitative thresholds, Art. 3(1), (2) DMA —	406
bb)	Designation procedure —	406
3.	Obligations of the gatekeepers —	408
a)	Duty to cooperate, Art. 3(3) DMA —	408
b)	Duties of conduct and omission, Art. 5–7 DMA —	408
c)	Obligations of gatekeepers in accordance with Art. 5 DMA —	409
aa)	Prohibition of data merging, Art. 5(2) DMA —	409
bb)	Prohibition of the processing of personal data for the purpose of operating online advertising services, Art. 5(2)(a) DMA —	409
cc)	Prohibition of merging personal data, Art. 5(2)(b) DMA —	410
dd)	Prohibition of re-use of personal data, Art. 5(2)(c) DMA —	410
ee)	Prohibition of circumvention by notification, Art. 5(2)(d) DMA —	411
ff)	Exceptions, Art. 5(2) DMA —	411
gg)	Prohibition of parity clauses, Art. 5(3) DMA —	412
hh)	Prohibition of anti-steering measures, Art. 5(4) DMA —	413

- ii) Access and use of content acquired elsewhere, Art. 5(5) DMA — **413**
- jj) Prohibition of obstruction of legal remedies, Art. 5(6) DMA — **414**
- kk) Prohibition of tying central platform services with selected other services, Art. 5(7), (8) DMA — **415**
- ll) Right to information, Art. 5(9), (10) DMA — **415**
- d) Obligations of gatekeepers in accordance with Art. 6 DMA — **416**
 - aa) Prohibition of data use, Art. 6(2) DMA — **417**
 - bb) Obligation to uninstall, Art. 6(3) DMA — **417**
 - cc) Interoperability of software applications and ‘app stores’, Art. 6(4) DMA — **418**
 - dd) Prohibition of self-preferential treatment with regard to rankings, Art. 6(5) DMA — **419**
 - ee) Switching options for end users, Art. 6(6) DMA — **419**
 - ff) Interoperability of operating systems and virtual assistants, Art. 6(7) DMA — **420**
 - gg) Making advertising tools available, Art. 6(8) DMA — **420**
 - hh) Obligations to provide access to data, Art. 6(9), (10), (11) DMA — **421**
 - ii) Access for commercial users under FRAND conditions, Art. 6(12) DMA — **422**
 - jj) Terms of cancellation, Art. 6(13) DMA — **423**
 - kk) Further obligations — **423**
- 4. Supervision and enforcement, Art. 20–43 DMA — **424**
 - a) Public Enforcement — **424**
 - b) Sanction options, Art. 20 et seqq. DMA — **425**
 - aa) Order to pay a fine, Art. 30 DMA — **425**
 - bb) Penalty payments, Art. 31 DMA — **426**
 - cc) Systematic non-compliance, Art. 18 DMA — **426**
 - dd) Provisional measures, Art. 24 DMA — **427**
 - ee) Investigative powers of the European Commission, Art. 21 et seq. DMA — **427**
 - c) Private enforcement — **427**
 - aa) Requirements for enforcement under private law and applicable regulations — **428**
 - bb) Practical relevance of private enforcement — **429**
- 5. Summary and implications for practice — **430**
 - a) Criticism regarding the appointment of gatekeepers — **430**
 - b) Criticism regarding the prohibition of data merging (Art. 5(2) DMA) — **432**
 - c) Outlook — **433**