

Table of contents

Preface to the English translation	V
List of abbreviations	XXI
List of literature	XXV

Part I

Basics

Chapter 1

Timeline of the AI Act

(Schwartmann/Kurth)

Chapter 2

Definitions

(Keber/Zenner/Hansen/Schwartmann)

A. Artificial intelligence	5
B. Symbolic AI (1 st Wave)	5
C. Machine Learning (2 nd Wave)	6
D. GPAI Models and Generative AI	7
E. Future prognosis (3 rd Wave)	7

Chapter 3

Differentiation from other fields of action

(Benedikt/Keber)

A. Differentiation from legal tech and automation	9
B. Differentiation from robotics	9

Chapter 4

Technical and economic classification of artificial intelligence

A. How AI applications work (<i>Meding</i>)	11
B. Overview of AI application areas and use cases	13
I. GPAI models and generative AI as co-pilots <i>(Schwartmann/Mühlenbeck)</i>	13
II. GPAI Models and Generative AI for Image and Text Processing <i>(Schwartmann/Mühlenbeck)</i>	14
III. Open-source and generative AI (<i>Wünschelbaum</i>)	15

IV.	Legal Tech und Smart Contracts (<i>Schwartmann/Mühlenbeck</i>)	17
V.	AI in legal, tax and management consulting (<i>Kremer</i>)	17
	1. AI as a product in its own right, as a service or integration into consulting services	17
	2. Practical examples of the use of AI in consulting services	18
	3. Short assessment in compliance with the AI Act	19
VI.	AI applications in sport and health sector (<i>Schwartmann/Mühlenbeck</i>)	19
VII.	AI in public sector	25
	1. Criminal prosecution (<i>Hartmann</i>)	20
	a) Specific use cases of law enforcement	21
	b) General Use Cases of Law Enforcement	22
	2. Educational institutions (<i>Schwartmann</i>)	22
	a) Starting point	22
	b) Assessment	23
	3. Authorities (<i>Wünschelbaum</i>)	23
VIII.	AI in the context of employment (<i>Wünschelbaum</i>)	25
IX.	Risk of circumvention by legacy systems (<i>Wünschelbaum</i>)	27

Part II Regulation of AI

Chapter 1 AI Act

A.	History of the law (<i>Zenner</i>)	31
B.	Scope of application	33
I.	Material scope of application (<i>Keber/Zenner</i>)	35
	1. Concept of artificial intelligence in the AI Act	35
	a) AI system	35
	b) GPAI models	36
	2. Protected legal interests	36
II.	Personal scope of application (<i>Keber/Zenner</i>)	37
	1. Obligated parties	37
	2. Protected parties	38
III.	Territorial scope of application (<i>Keber/Zenner</i>)	39
IV.	Scope exceptions	40
	1. Free and open-source licence (FOSS) (<i>Keber/Zenner</i>)	40
	a) Development	40
	b) AI systems, not models	40
	c) Free and open-source licence (FOSS)	40
	d) Provided	41
	2. GDPR (<i>Maslewski</i>)	41
	3. Research (<i>Keber/Zenner</i>)	42
	4. Military (<i>Keber/Zenner</i>)	43
	5. Further exceptions (<i>Schwartmann/Köhler</i>)	44

C. Risk-based approach	47
I. Basics (<i>Schwartmann/Köhler</i>)	47
II. Measures for AI literacy (Art. 4) (<i>Schwartmann/Köhler</i>)	48
III. Prohibited AI systems	49
1. Subliminal influence (Art. 5 para. 1 letter a) (<i>Schwartmann/Pottkämper</i>)	49
a) Purpose and scope of application	49
b) Definition and scope for interpretation	49
c) Conditions for the prohibition	49
d) Limitations and future considerations	50
2. Exploiting of vulnerabilities and other weaknesses (Art. 5 para. 1 letter b) (<i>Schwartmann/Pottkämper</i>)	50
a) Aim and scope	50
b) Restrictions and effects	50
c) Future developments	51
3. Evaluation based on social behaviour (Art. 5 para. 1 letter c) (<i>Schwartmann/Pottkämper</i>)	51
a) Prohibition and its conditions	51
b) Objective and challenges	51
c) Specification of the prohibition	52
d) Scope of application and future considerations	52
4. Predictive policing (Art. 5 para. 1 letter d) (<i>Schwartmann/Keber/Köhler</i>)	52
a) Scope of application	53
b) Risks of predictive policing	54
c) Differentiation from automated data analysis	54
5. Untargeted collection and use of facial images (Art. 5 para. 1 letter e) (<i>Schwartmann/Keber/Pottkämper</i>)	55
6. Emotion recognition systems (Art. 5 para. 1 letter f) (<i>Schwartmann/Keber/Steinbrück</i>)	56
7. Biometric categorisations (Art. 5 para. 1 letter g)	58
8. Biometric real-time remote identification (Art. 5 para. 1 letter h) (<i>Ganter/Rembold</i>)	59
a) Prohibition of use	59
b) The authorised purposes of the use of RBI	60
aa) Search for victims of criminal offences and missing persons (Art. 5 para. 1 subpara. 1 letter h point i)	60
bb) Defence against serious threats (Art. 5 para. 1 subpara. 1 letter h point ii)	60
cc) Investigation of criminal offences (Art. 5 para. 1 subpara. 1 letter h point iii)	60
dd) Purposes other than law enforcement (Art. 5 para. 1 subpara. 2)	61
c) Further requirements for the RBI (Art. 5 para. 2)	61
aa) Situation impact assessment (Art. 5 para. 2 subpara. 1 letter a)	61

bb) Intervention impact assessment (Art. 5 para. 2 subpara. 1 letter b)	61
cc) Appropriate restrictions, fundamental rights impact assessment and registration (Art. 5 para. 2 subpara. 2)	61
d) Authorisation of the RBI by national authorities (Art. 5 para. 3)	62
e) Notification to market surveillance authority and data protection authority (Art. 5 para. 4)	62
f) Implementation of the RBI in national law (Art. 5 para. 5)	63
g) Annual report of the market surveillance authorities and data protection authorities on the use of RBI (Art. 5 para. 6)	63
h) Annual report of the Commission on the use of RBI (Art. 5 para. 7)	63
9. Relationship to other Union law (Art. 5 para. 8)	64
IV. High-risk AI systems	64
1. Basics (<i>Schwartmann/Köhler</i>)	64
a) Classification according to Art. 6 para. 1	65
b) Classification according to Art. 6 para. 2	65
aa) Exceptions to the high-risk classification (Art. 6 para. 3)	65
bb) Right of the Commission to amend the relevant criteria	70
c) Right of the Commission to amend Annex III	70
2. High-risk AI systems pursuant to Art. 6 para. 1 (Annex I) (<i>Schwartmann/Pottkämper</i>)	71
a) Ways to be categorised as a high-risk AI system pursuant to Art. 6 para. 1 in conjunction with Annex I	72
b) High-risk AI systems in product safety law	72
c) Product regulation under the old legal framework	72
d) Product regulation under the new legal framework	73
e) Consequences of classification as a high-risk system	73
f) Interim conclusion	73
3. High-risk AI systems pursuant to Art. 6 para. 2 AI Act (Annex III)	74
a) Biometric identification, categorisation and emotion recognition of natural persons (<i>Hansen/Nägele/Steinbrück</i>)	74
b) Management and operation of critical infrastructures (<i>Nägele</i>)	76
c) Education and training	78
aa) High-risk classification according to Annex III no. 3 (<i>Schwartmann/Keber/Henning/Köhler</i>)	78
bb) Guidance for educational institutions (<i>Schwartmann</i>)	81
d) Employment, worker's management and access to self-employment (<i>Wünschelbaum</i>)	86
aa) Sectoral scope of application	86
bb) Covered employment areas	88
cc) Exemptions from high-risk regulation	89
e) Accessibility and utilisation of basic private and public services and benefits (<i>Schwartmann/Köhler</i>)	91
aa) Access to public support and services	92
bb) Creditworthiness and credit score	92
cc) Life and health insurance	93
dd) Emergency calls	94

f) Prosecution (<i>Benedikt/Hartmann</i>)	94
g) Migration, asylum and border control (<i>Benedikt</i>)	96
h) Administration of justice and democratic processes	97
aa) High-risk classification according to Annex III no.8 (<i>Schwartmann/Benedikt/Köhler</i>)	97
bb) Structured party submissions – a case for the AI Act? (<i>Schwartmann/Köhler</i>)	101
4. Requirements for high-risk AI systems	103
a) Compliance with the requirements for high-risk AI systems (Art.8) (<i>Schwartmann/Keber/Köhler/Zenner</i>)	103
aa) Genesis	103
bb) Addressees of the obligations	104
cc) Modalities of compliance	104
dd) Special features for AI systems within the meaning of Art.6 para.1	105
ee) Use case and competition with other obligations under the AI Act	105
b) Risk management system (Art.9) (<i>Hansen</i>)	106
aa) Management systems for dealing with risks	106
bb) Requirements of Art.9 for a risk management system	107
cc) Proof of fulfilment of Art.9 of the AI Act	110
c) Data and data governance (Art.10) (<i>Schwartmann/Keber/Köhler/Nägele</i>)	110
aa) Regulation of training, validation and test data sets (Art.10 para.1–4 AI Act)	112
bb) Legal basis for the processing of special categories of personal data (Art.10 para.5 GDPR)	114
d) Technical documentation (Art.11 AI Act) (<i>Hansen</i>)	115
e) Record-keeping obligations (Art.12) (<i>Schwartmann/Keber/Köhler</i>)	117
aa) Logging functions to ensure traceability	117
bb) Special logging functions for biometric remote identification systems	118
cc) Addressee and retention obligation	118
dd) Conflict with judicial independence	119
f) Transparency and provision of information to deployers (Art.13) (<i>Schwartmann/Keber/Köhler</i>)	119
aa) Importance of transparency in the use of high-risk AI systems	120
bb) Transparency	120
cc) Operating instructions	121
g) Human oversight (Art.14) (<i>Schwartmann/Keber/Köhler</i>)	122
aa) Understanding of functioning and risks (Art.14 para.4 letters a–c)	123
bb) Interference with the business (Art.14 para.4 letters d and e)	124
cc) Verification when using biometric remote identification systems	125

h) Accuracy, robustness and cybersecurity (Art. 15 AI Act) (Nägele/Steinbrück)	125
5. Obligations in dealing with high-risk AI systems (Kremer/Haar) ...	128
a) Obligations of providers of high-risk AI systems (Art. 16–22 AI Act)	128
aa) General obligations of providers (Art. 16 AI Act)	128
bb) Existence of a quality management system (Art. 17 AI Act)	129
cc) Documentation keeping (Art. 18 AI Act)	130
dd) Retention of the logs (Art. 19 AI Act)	131
ee) Taking corrective actions and duty of information (Art. 20 AI Act)	132
ff) Cooperation with competent authorities (Art. 21 AI Act) ...	133
gg) Appointment of an authorised representative (Art. 22 AI Act)	134
b) Obligations of importers of high-risk AI systems (Art. 23 AI Act) ...	136
aa) Inspection obligations (para. 1, para. 2)	136
bb) Obligations from placing on the market (para. 3–5)	137
cc) Cooperation with the competent authorities (para. 6, para. 7) ...	137
c) Obligations of distributors of high-risk AI systems (Art. 24 AI Act)	138
aa) Inspection obligations (para. 1, para. 2)	138
bb) Obligations from making available on the market (para. 3–4) ...	138
cc) Cooperation with the competent national authorities (para. 5, para. 6)	139
d) Obligations of deployers of high-risk AI systems (Art. 26 AI Act)	139
aa) Obligations in connection with use (para. 1–3)	139
bb) Appropriate and representative input data (para. 4)	140
cc) Monitoring obligations (para. 5)	141
dd) Obligation to retain automatically generated logs (para. 6)	141
ee) Information obligation for employers (para. 7)	142
ff) Registration (para. 8)	142
gg) Carrying out the data protection impact assessment (para. 9) ...	142
hh) High-risk AI system for post-remote biometric identification (para. 10)	143
ii) Duty to provide information to natural persons (para. 11)	144
jj) Cooperation with the competent national authorities (para. 12)	144
e) Fundamental rights impact assessment for high-risk AI systems (Art. 27 AI Act)	144
aa) Deployers obliged to carry out the fundamental rights impact assessment (para. 1)	145
bb) Timing, frequency of implementation and relationship to the data protection impact assessment (para. 1, para. 2, para. 4)	145
cc) Subject of the fundamental rights impact assessment (para. 1)	145
dd) Notification to the market surveillance authority (para. 3, para. 5)	146

V. AI systems with special transparency obligations (Art. 50 AI Act)	
(Kremer/Haar)	146
1. Time of fulfilment of the transparency obligations (para. 5)	146
2. Conformity with the applicable accessibility requirements (para. 5)	147
3. Special transparency obligations	147
a) AI systems intended to interact directly with natural persons	
(para. 1)	147
b) AI systems generating synthetic audio, image, video or text	
content (para. 2)	148
c) Emotion recognition systems or biometric categorisation systems	
(para. 3)	149
d) AI systems for the generation of deep fakes (para. 4 case 1)	149
e) AI system for generating or manipulating texts to inform the	
public (para. 4 case 2)	150
4. Relationship of the special transparency obligations to the Digital	
Services Act	150
VI. Simple AI systems (Art. 2 in conjunction with Art. 112, Art. 95)	
(Kremer/Haar)	151
D. Responsibilities along the AI value chain (Zenner/Schwartmann/Hansen)	151
I. The conceptual problems with the Commission's regulatory approach	151
II. Overview of the final approach after the dialogue	153
1. GPAI models with systemic risk (Level 1) (Art. 51 and 52 AI Act)	155
a) Genesis	155
b) Definitions of GPAI models (Art. 3 no. 63–65)	156
c) Classification of systemic GPAI models (Art. 51 and 52 AI Act)	156
d) GPAI models with systemic risk (Art. 51 AI Act)	156
e) Notification obligation under Art. 52 para. 1 AI Act	157
f) Information and documentation obligations for systemic GPAI	
models under Art. 53 of the AI Act	158
g) Specific obligations for GPAI models with systemic risk (Art. 55	
AI Act)	158
h) Codes of Practice (Art. 56 AI Act)	158
2. GPAI models and AI components (Level 2) (Art. 53 and Art. 25	
para. 2 AI Act)	160
3. Provider (Level 3)	162
a) Definition	163
b) Provider change through actions listed in Art. 25 AI Act	
("upgrade with consequences")	163
aa) Trademark (Art. 25 para. 1 letter a)	163
bb) Technical modification (Art. 25 para. 1 letter b)	164
cc) Change of the intended purpose (Art. 25 para. 1 letter c)	164
dd) Cooperation (Art. 25 para. 2 AI Act)	164
4. Deployer (Level 4)	165
5. Affected person (level 5)	166

E. Harmonised standards and common specifications (Art.40 et seq. GDPR)	
<i>(Hansen)</i>	166
I. European standardisation	167
II. Role of standardisation in the AI Act	168
III. Harmonised standards and standardisation documents (Art. 40 AI Act)	169
IV. Common specifications (Art.41 AI Act)	170
F. Regulatory sandboxes (Art.57 et seq. AI Act) (Keber/Hansen/Nägele)	170
I. General	170
II. Aims of the regulatory sandboxes	171
III. Implementing acts of the Commission	172
IV. Authorisation for further processing of personal data	172
V. Final report	173
VI. Liability	174
VII. Testing under real conditions outside of AI regulatory sandboxes ...	174
VIII. Promoting innovation, especially among SMEs and start-ups	175
IX. National Regulatory Sandbox Act	176
X. Applicable regulations for health research with AI	176

Chapter 2

National regulation

(Schwartzmann/Köhler)

A. Scope of application of the AI Act	177
B. Opening clauses	178
C. Permissibility of the use of AI systems	178
D. Use case: AI use in the media	180
I. Differentiation according to automation levels	180
II. Special problem: Ensuring diversity in the use of AI in the media	182

Chapter 3

Relationship with other areas of law

A. Data law	183
I. GDPR	183
1. Scope of application and responsibility <i>(Schwartzmann/Köhler)</i>	183
a) Data categories in dealing with AI systems	184
b) Applicability of the GDPR	184
c) Responsibility under data protection law	185
2. Concept of artificial intelligence in the GDPR <i>(Maslewski)</i>	186
3. Prohibition with reservation of authorisation pursuant to Art. 6 para. 1 and Art. 9 para. 1 GDPR <i>(Keber)</i>	187
a) Consent (Art.6 para. 1 letter a GDPR)	188

b) Necessary for the performance of a contract (Art. 6 para. 1 letter b GDPR)	188
c) Necessary for compliance with a legal obligation (Art. 6 para. 1 letter c GDPR)	189
d) Public interest or public authority (Art. 6 para. 1 letter e GDPR)	189
e) Legitimate interests (Art. 6 para. 1 letter f GDPR)	189
f) Change of purpose (Art. 6 para. 4 GDPR)	191
4. Special categories of personal data (<i>Keber/Steinbrück</i>)	191
5. Prohibition of automated individual decision-making pursuant to Art. 22 GDPR (<i>Schwartmann/Benedikt/Köhler</i>)	192
6. Transparency and information obligations pursuant to Art. 5 para. 1 letter a and 12 et seq. GDPR (<i>Schwartmann/Köhler</i>)	194
7. Technical and organisational measures (Art. 24, 25, 32 GDPR) (<i>Hansen/Keber</i>)	196
a) Requirements of the GDPR	196
aa) Objective of the technical and organisational measures in the GDPR	197
bb) Requirements of Art. 25 GDPR: Organisation of the processing	197
cc) Requirements of Art. 32 GDPR: Security of processing	198
b) Significance for AI systems	199
aa) General	199
bb) Implementation of Art. 25 GDPR in relation to AI systems	199
cc) Implementation of Art. 32 GDPR in relation to AI systems	201
c) Guidelines and standards	202
d) DSK guidance for the data protection-compliant use of AI applications	202
II. BDSG and German federate states' data protection laws (<i>Schwartmann/Köhler</i>)	203
1. German Federal Data Protection Act (BDSG)	203
2. Federate states' data protection laws	204
III. Telecommunication Digital Services Data Protection Act (TDDDG) (<i>Benedikt</i>)	204
IV. Data Act (DA) (<i>Schwartmann/Wasilewski</i>)	205
1. General considerations between AI Act and DA	206
2. Data and data governance (Art. 10 AI Act)	207
V. Data Governance Act (DGA) (<i>Schwartmann/Pottkämper</i>)	208
1. Addressees	208
2. Main contents of the legal acts	209
a) AI Act: Safety and responsibility in the use of AI	209
b) Data Governance Act: data availability and exchange	209
c) Complementary relationship between AI Act and DGA	209
VI. European Data Spaces (<i>Schwartmann/Wasilewski</i>)	210
1. European Health Data Space (EHDS)	210
2. "GreenData4All"	213

B. Relationship with other European legal acts (Schwartzmann/Wasilewski)	214
I. European Media Freedom Act (EMFA)	214
II. Other legal acts	215
C. Copyright (Sänger)	216
I. The input side	216
1. Copyright in training data	216
2. Prompts	219
II. The output side	220
1. No copyright for the AI application	220
2. Copyright of the provider	220
3. Copyright of the user	221
4. Related property rights	221
D. Personal rights (Schwartzmann/Köhler)	223
I. Violations of personal rights through AI-generated content	223
II. Approaches to solutions in development	225
III. Consequences for users	226
E. Exam regulation (Schwartzmann/Köhler/Kurth)	226
I. Use of AI systems on the part of the candidates	227
II. Use on the part of the examiners	228
F. Labour law: AI in the employment context (Wünschelbaum)	229
I. Employment-specific AI prohibitions	230
II. Employer as provider and deployer	231
III. Employees as deployers	232
IV. AI opening clause in the employment context	233
1. Purpose	234
2. Personal scope: Employees and partly solo self-employed persons	234
3. Material scope of regulation: user sphere	234
4. Permissible regulatory instruments	235
a) Laws	235
b) Collective agreements	235
c) Concept of "more favourable" regulation	236
aa) Multidimensional regulatory objectives	236
bb) More favourable means advantages without falling below the level of protection	237
5. Legal scope for regulation	237
a) Specification of high-risk systems in accordance with Annex III no. 4	238
b) Implementation of the Platform Directive	238
c) AI Officer	239
d) Clarify the employer's deployer status	239
e) Strengthening the rights of employees	239
f) Sandboxing options and regulatory sandboxes for deployers in the employment context	240
g) Cross-border use of AI systems	240

6. Scope for regulation in collective agreements	240
a) Use of AI in the Group	241
b) Concretisation of requirements: Participation and information rights of the AI Act	241
V. Regulatory competition in Union law: Platform Directive	242
VI. Competing regulations in German labour law	242

Part III Enforcement

Chapter 1 Governance

A. Introduction (Zenner)	247
B. Overview of governance structures	248
I. Commission (AI Office, Art. 64 et seq.) (Zenner)	248
II. European Artificial Intelligence Board (Art. 65–66 AI Act) (Zenner)	250
III. Advisory forum (Art. 67 AI Act) (Zenner)	250
IV. Scientific Panel of Independent Experts (Art. 68–69 AI Act) (Zenner)	251
V. European Data Protection Supervisor (EDPS) (Zenner)	251
VI. Evaluation (Zenner)	251
VII. National authorities (Schwartzmann/Hansen/Keber)	252
1. Structure	252
a) National authorities under the AI Act	252
b) Assignment to national authorities	254
2. Obligations of the Member States	256
3. Modalities of the supervision	257
a) Independence, impartiality and without bias	257
b) Confidentiality	257
c) Exchange of experience	257
d) Guidance and advice	257
VIII. Catalogue of measures (Schwartzmann/Keber/Zenner/Hansen)	257
1. Market surveillance authorities	258
a) Investigative powers	258
b) Supervisory measures in the event of violations of the AI Act	259
c) Other tasks of the market surveillance authorities	260
2. Other national authorities (Art. 77 AI Act)	260
3. GPAI systems and models	261
IX. Notification procedure and notified bodies (Schwartzmann/Köhler) ...	262
X. Legal remedies (Schwartzmann/Köhler)	263
1. Right to lodge a complaint with a competent market surveillance authority (Art. 85 AI Act)	263
2. Right to explanation of the individual decision-making (Art. 86 GDPR)	264
3. Whistleblower directive	264

Chapter 2

Liability

A. Basics	<i>(Kessen)</i>	265
I.	Contractual liability	266
II.	Tortious liability	267
1.	Liability of the user/operator	267
2.	Liability of manufacturers and suppliers	270
a)	Product Liability Act	270
b)	Producer liability	271
c)	Liability according to Section 823 para.2 BGB	272
B. Special issues of national law		273
I.	Liability for copyright infringements <i>(Sänger)</i>	273
1.	Inputs	273
2.	Outputs	274
II.	Liability for violations of personal rights <i>(Schwartzmann/Köhler)</i>	275

Chapter 3

Sanctions and other enforcement measures

(Schwartzmann/Köhler)

A. Fines	277
I.	General conditions
II.	Amount of the fines
III.	Special features for GPAI models and Union bodies
IV.	Fines under the GDPR
B. Other sanctions and enforcement measures	279

Chapter 4

Official orders under the GDPR

(Keber/Maslewski)