

# Index

The references start with the part, the following bold numbers signify the chapters, the meagre ones the paragraphs.

**1<sup>st</sup> Wave** **I 2 2**

**2<sup>nd</sup> Wave** **I 2 6**

**3<sup>rd</sup> Wave** **I 2 8**

**Abstract threat** **II 1 92**

**Access to high-quality data** **II 3 86**

**Access to self-employment** **II 1 202 f.**

**Accuracy** **II 1 356**

**Ad Hoc Committee on Artificial Intelligence (CAHA)** **II 1 52**

**Adaptable regulation** **II 1 204**

**Adjustment periods** **I 4 65**

**Administration of justice** **II 1 246 f.**

**Administrative offence** **III 2 26**

**AI**

– as a product **I 4 24**

– as a service **I 4 24**

– definition GDPR **II 3 16**

– integration in consulting **I 4 24**

**AI Act**

– catalogue of sanctions **III 3 14**

– civil liability **III 2 1**

– competing regulations in German labour law **II 3 193**

– contractual liability **III 2 7**

– Data Act **II 3 82**

– data and data governance **II 3 84**

– employer as subject to provider obligations **II 3 160**

– ex-ante conformity assessment **III 1 20**

– ex-post surveillance **III 1 19**

– implementation of GDPR **II 3 67**

– national authorities **III 1 18**

– national regulation **II 2 1**

– presumption of conformity **II 1 552**

– protected parties **II 1 24**

– relationship with other areas of law **II 3 1**

– scope of application **II 2 3**

– technology-related minimum level of protection **II 2 11**

– tortious liability **III 2 8**

**AI and cybersecurity** **II 1 175**

**AI application**

– copyright **II 3 125**

**AI as a product** **I 4 24**

**AI assistance systems in the judiciary** **II 1 253**

**AI HLEG** **II 1 308**

**AI in employment context** **II 3 155**

– additional provider obligations **II 3 160**

– collective agreements **II 3 165, 188**

– competing regulations in German labour law **II 3 193**

– cross-border use **II 3 187**

– General Act on Equal Treatment **II 3 194**

– legal and administrative provisions **II 3 165**

– minimum harmonisation **II 3 166**

– opening clause **II 3 169**

– participation and information rights **II 3 191**

– participation rights of works council **II 3 196, 198**

– prohibition system **II 3 156**

– protection of employees' rights **II 3 165**

– use in the group **II 3 190**

– user sphere **II 3 169**

**AI in examinations** **I 4 46**

**AI in the context of employment** **I 4 55, 60**

**AI literacy** **II 1 55, 188, 200, 307, 340**

– general responsibility **II 1 192**

– legal obligation to impart **II 1 55**

– specific responsibility **II 1 192**

**AI Office** **III 1 44**

**AI officer** **II 3 183**

**AI output**

– direct control **II 3 143**

– fictional characters **III 2 29**

– in the style of certain artists **III 2 31**

– manga figurine **III 2 29**

– novel **III 2 29**

– protection rights **II 3 135**

**AI product regulation** **II 2 11**

**AI products** **II 1 483**

**AI regulatory sandboxes** **II 1 540**

**AI selection**

– economically **I 4 1**

– technical **I 4 1**

**AI start button** **II 1 201**

**AI system** **I 4 26, 31; II 1 12, 28**

– adaptility **II 1 14**

– application process **II 3 194**

– applications for organising and structuring existing databases **II 1 85**

– assessment of an appropriate level of education **II 1 180**

– cross-border use **II 3 187**

– data processing **II 3 17, 79**

– developement **II 3 17**

– direct interaction with natural persons **II 1 458**

– discrimination on the grounds of age **II 1 64**

– distributor **II 1 21**

- Dual Use II 1 41
- emotions II 1 89
- generating texts to inform the public II 1 473
- generation of deepfakes II 1 469
- importer II 1 21
- intentions of natural persons II 1 89 f.
- manipulation of texts to inform the public II 1 473
- military tasks II 1 206
- OECD definition II 1 12 f.
- output II 3 48
- permissibility of use II 2 9
- phases of training and validation II 3 48
- pure information III 2 23
- putting into service II 1 64
- putting into use II 1 64
- research II 1 36
- state as provider I 4 49
- technical and organisational measures II 3 61
- technology-related opacity II 3 34
- use II 1 64; II 3 17
- wording of the prohibition II 1 72
- AI system in the judiciary** II 1 252 f., 255
  - basic document II 1 261
  - constitutional limits II 1 265
  - court as deployer of a high-risk AI systems II 1 264
  - judge-machine-judge II 1 255
  - lawyer's freedom II 1 263
  - start button II 1 255
  - stop button II 1 255
  - structured party submission II 1 261
  - support of judicial decision-making II 1 253
- AI systems for generating synthetic audio, image, video or text content** II 1 462
- AI systems for the generation of deepfakes** II 1 469
- AI systems with special transparency obligations** II 1 450
  - applicable accessibility requirements II 1 456
  - time of fulfilment II 1 453
- AI use in the media** II 2 12, 17
  - ensuring diversity II 2 17
- AI value chain** II 1 273
- AI-forecast system** II 1 85
- AI-generated files** II 3 80
- Aims of regulatory sandboxes** II 1 546
- Alternative dispute resolution** II 1 256
- Anchor effect** II 1 200, 251
- Ancillary protection rights**
  - AI-generated journalistic content II 3 133
- Anomaly detection** II 1 175
- Anomaly detection systems** II 1 173
- Anonymisation** II 1 250
- Anticipation of the violation of personal rights** II 3 141
- Applicability of GDPR** II 3 7
- Applicant Tracking-Systems (ATS)** I 4 56
- Application**
  - AI I 4 11
  - Use Cases I 4 11
- Appointment of authorised representative** II 1 393
- Appropriate and representative input data** II 1 421
- Appropriate level of protection** II 1 354
- Appropriate Technical and Organisational Measures (TOM)** II 3 50
- Artificial intelligence**
  - definition II 1 11
- Assessment**
  - of applicants II 1 212
- Assessment List for Trustworthy Artificial Intelligence (ALTAI)** II 1 308
- Assistance system** II 2 14
- Asylum** II 1 242, 244
- Asylum applications**
  - AI-based assessment of identity II 1 242
- Asylum Procedures Directive** II 1 245
- Attention Head** I 4 7
- Authorisation for further processing of personal data** II 1 550
- Authorisation of RBI**
  - by national authorities II 1 114
- Authorities**
  - confidentiality III 1 27
  - principles III 1 26
- Automated analysis of digitised works** II 3 113
- Automated data analysis** II 1 83
- Automated data processing**
  - admissibility II 1 85
  - danger II 1 85
- Automation** I 3 1
- Automation bias** II 1 81, 200, 251, 344, 349; II 3 140
- Automation levels** II 2 13
- Autonomous vehicles** II 3 80
- Autonomy** II 1 14, 71
- Backpropagation algorithm** I 4 3
- BDSG** II 3 71 f.
- Benchmarks and measurement methods** II 1 358
- Betriebsanleitung** II 1 335
- Bias** II 1 299
- Biometric categorisation**
  - categorisation systems II 1 97
- Biometric categorisation system** II 1 466
- Biometric data** II 1 90
- Biometric identification** II 1 99
- Biometric real-time remote identification** II 1 100
- Black box** II 1 483

- Border control** II 1 242, 244  
**Broadcast programme** II 3 130  
**BSI** II 1 360
- Catalogue of criteria** II 1 130  
**Catalogue of fines** III 3 2  
**CE marking** II 1 410  
**CEN** II 1 360  
**CENELEC** II 1 360, 527  
**Certificate** II 1 363  
**Change of purpose** II 3 32  
**ChatGPT in teaching** II 1 188  
**Circumvention strategy** I 4 66  
**Civil liability** III 2 1  
**Classroom analytics** II 1 182  
**Closed systems** II 3 70  
**Cloud switching** II 3 81  
**Codes of Conduct** II 3 69  
**Cognitive biases** II 1 251  
**Combination and linking possibilities** II 3 33  
**Commission guidelines** II 1 220  
**Common specification** II 1 525, 531 f., 538  
**Comparison of collected biometric data** II 1 103  
**Competition rules** II 1 44, 48  
**Compliance** I 4 28  
 – data protection II 3 18  
**Compliance management** II 1 213  
**Compliance with data protection requirements** II 1 551  
**Compliant risk products** III 1 41  
**Concept of risk** II 1 53  
**Conformity assessment body** II 1 127  
**Conformity assessment procedure** III 1 51  
**Consulting** I 4 24  
**Consumer protection** II 1 48  
**Cookies** II 3 80  
**Cooperation with competent authorities** II 1 388  
**Co-pilots** I 4 11  
**Copyright**  
 – AI application II 3 125  
 – AI-generated images II 3 131  
 – AI-generated music II 3 132  
 – AI-generated software II 3 125  
 – AI-generated speech II 3 132  
 – provider II 3 127  
 – related property rights II 3 130  
 – user II 3 128  
**Copyright in training data** II 3 112  
**Copyright law** II 3 112  
 – AI output in the style of certain artists III 2 31  
 – caricature III 2 30  
 – disclosure III 2 26  
 – distribution III 2 28  
 – fair use III 2 29  
 – input III 2 27  
 – notice III 2 26  
 – output III 2 28  
 – parody III 2 30  
 – pastiche III 2 30  
 – public availability III 2 28  
 – reproductions III 2 28  
**Corporate liability** III 3 5  
**Court** II 1 249  
**Court disputes** I 4 28  
**Credit score** II 1 225  
**Creditworthiness** II 1 225; II 3 40  
**Criminal justice** II 1 236  
**Criminal offence** III 2 26  
**Critical infrastructures** II 1 172, 174  
**Customer management** I 4 28  
**Cybercrime in the broader sense** I 4 35  
**Cybercrime in the narrower sense** I 4 35  
**Cybersecurity** II 1 353, 356; III 1 27  
 – accuracy and robustness II 1 353  
 – data quality and data quantity II 1 356
- Damage**  
 – immaterial II 1 281  
 – material II 1 281  
**Data** II 1 297  
 – body temperature II 1 91  
 – error-free II 1 303  
 – gait II 1 91  
 – garbage in, garbage out II 1 297  
 – gaze direction II 1 91  
 – gestures II 1 91  
 – heart rate II 1 91  
 – keystrokes II 1 91  
 – relevant II 1 303  
 – representative II 1 303  
 – skin conductivity II 1 91  
 – voice II 1 91  
**Data Act (DA)** II 3 81  
 – making data accessible and sharing II 3 85  
**Data altruistic organisations** II 3 88  
**Data augmentation** II 3 63  
**Data categories in dealing with AI systems** II 3 4  
**Data Ethics Commission** II 2 18; III 1 30  
**Data governance** II 1 297, 536  
**Data Governance Act (DGA)** II 3 87, 91, 162  
**Data intermediation services** II 3 88  
**Data law** II 3 3  
**Data poisoning** II 1 175, 359  
**Data protection compliance of the controller** II 3 18  
**Data protection impact assessment** I 4 28; II 1 431  
**Data protection management systems (DSMS)** II 1 278

- Data protection supervisory authorities as market surveillance authorities** III 1 22
- Data quality** II 3 33
- Data quality and data quantity** II 1 356
- Databases** II 3 133
- De facto machine decision** II 1 201
- Decision**
  - term II 1 220
- Decision process**
  - transparency and accountability I 4 53
- Declaration of conformity** II 1 363
- Deep Learning** I 2 6
- Deep neural network** I 4 3
- Defense policy** II 1 41
- Definition of AI**
  - GDPR II 3 16
- Delegated act** II 1 145
- Delegation** II 2 15
- Delegation acts** II 1 205
- Demarcation criteria** II 3 11
- Democratic processes** II 1 246, 259
- Deployer**
  - responsibility for professional purposes II 3 164
- Deployer in employment context** II 3 186
- Design error** III 2 22
- Detrimental treatment** II 1 70
- Developer's servers** II 3 14
- Digital divide** II 1 183
- Digital Markets Act (DMA)** II 3 107
- Digital Services Act (DSA)** II 1 48, 170; II 3 107
- Digitalisation of crime** I 4 35
- DIN** II 1 360
- Directive AI-Liability**
  - draft III 2 16
- Discrimination** II 1 299
- Discriminative AI** I 4 33
- Discriminatory decisions** I 4 58
- Disproportionate negative consequences** II 1 70
- Distribution of training data** II 3 137
- Distributor** II 1 21, 409
  - inspection obligations II 1 410
- Diversity** II 2 17
- Diversity of opinion**
  - safeguard II 2 18
- Documentation** II 2 8
  - clear and comprehensible form II 1 311
  - retention period II 1 373
  - simplified form for SMEs II 1 313
- Documentation obligation** III 2 10
- Drones for military purposes** II 1 41
- DSK guidance** II 3 70
- Dual-Use AI systems** II 1 41
- Dual-use technology** II 1 355
- Dublin-III-Regulation** II 1 245
- Duties of care** III 2 10, 12
- Economic harm** II 1 66
- Education** I 4 42; II 1 176
  - support of text production II 1 183
- Educational institutions** II 1 185
- Election** II 1 259
- Electronic health data**
  - non-discriminatory access II 3 96
  - primary use II 3 95
  - scientific research II 3 99
  - secondary use II 3 95
  - training of AI systems II 3 96
  - unauthorised secondary use II 3 98
- Emergency calls** II 1 230
- Emergency first response services** II 1 230
- Emotion recognition system** II 1 89, 466
- Employee excess** II 3 164
- Employee protection** II 2 5
- Employees as deployers** II 3 164
- Employer's deployer status** II 3 184
- Employment** II 1 202f., 206, 219
- Employment context** II 1 202
- Employment relationships** II 1 208
- Employment sector** I 4 55
- Enforcement measures** III 3 1, 14
- Environmental data** II 3 104
  - accessibility II 3 104
  - shared use II 3 104
- Error of commission** II 1 344
- Escape into private use** II 1 47
- Establishment of regulatory sandbox**
  - competent authorities II 1 542
- Ethics** II 1 307
- ETSI** II 1 360
- EU declaration of conformity** II 1 395
- EU product safety legislation** III 1 24
- European Commission's White Paper on Artificial Intelligence** II 1 52
- European Data Spaces** II 3 93
- European data strategy** II 3 81, 93
- European Fundamental Rights Agency** II 1 82
- European Health Data Space (EHDS)** II 3 95
- European Media Freedom Act (EMFA)** II 3 106
- European Telecommunications Standards Institute** II 1 527
- European Union Agency for Cybersecurity (ENISA)** II 1 175
- Evaluation**
  - of learning outcomes II 1 189
- Evidence** II 1 232; III 2 16
- Exam** I 4 43
- Exam regulation** II 3 145
  - use on part of the candidates II 3 146
  - use on part of the examiner II 3 150
- Examination** I 4 42
- Examination assessment** I 4 42
- Exceptions** II 1 44
  - development activities II 1 46

- personal and non-professional activities II 1 47
- research activities II 1 46
- testing activities II 1 46
- Exceptions to the scope** II 1 26
- Exceptions to the scope of application** II 1 7, 44
- Exchange of experience** III 1 28
- Expert systems** I 2 3; I 4 62
- Explainable Artificial Intelligence (XAI)** II 3 64
- Exploitation**
  - age II 1 64
  - disability II 1 64
  - economic situation II 1 64
  - social situation II 1 64
- Exploitation of vulnerabilities of certain groups** II 1 64
- Exploitation of vulnerabilities of certain individuals** II 1 64
- Expression of emotion** II 1 92
- F13** I 4 48
- Facial images** II 1 86
- Fake news** II 3 110
- Federal Carel Office** III 1 21
- Federal Labour Court** II 3 198
- Federal Network Agency** III 1 21
- Federate states' data protection laws** II 3 75
- Final decision** II 1 254
- Fines**
  - amount III 3 7f.
  - GDPR III 3 13
  - parent company III 3 9
- Forbidden subliminal influence** II 1 58
- FOSS-AI system**
  - privileged treatment II 1 33
- Foundation Model** II 1 16
- Frauke** I 3 1
- Free and open-source licence (FOSS)** I 4 18; II 1 26, 29
- Full harmonisation**
  - exception II 2 9
- Fully autonomous assumption of tasks** II 2 16
- Fundamental rights impact assessment** I 4 53; II 1 193
- Fundamental rights impact assessment for high-risk AI systems** II 1 442
  - frequency of implementation II 1 444
  - notification to market surveillance authority II 1 449
  - obliged parties II 1 443
  - relationship to data protection impact assessment II 1 444
  - subject II 1 447
  - timing II 1 444
- Further processing for different purpose** II 1 550
- GDPR** II 1 35
  - automated data processing II 3 36f.
  - availability and resilience II 3 57
  - compliance with a legal obligation II 3 23
  - consent II 3 20
  - data protection principles II 3 51, 55
  - exclusivity II 3 41
  - fines III 3 13
  - guidelines and standards II 3 69
  - implementation in relation to AI systems II 3 67
  - implementation of AI systems II 3 62
  - implementation of the GDPR II 3 62
  - implementation of the rights of data subjects II 3 65
  - input data II 3 45
  - integrity and confidentiality II 3 57
  - legal effects II 3 38
  - legitimate interests II 3 25
  - necessity II 3 56
  - non-personal training and validation data II 3 63
  - objective of the technical and organisational measures II 3 51
  - official orders III 4 1
  - overall view of the processing of personal data II 3 53
  - performance of a contract II 3 21
  - powers of authorisation III 4 1
  - powers of investigation III 4 1
  - processing technology II 3 33
  - prohibition of automated individual decision-making II 3 35
  - public authority II 3 24
  - public interest II 3 24
  - remedial powers III 4 1f.
  - requirements of the organisation of the processing II 3 54
  - revocability of consent II 3 20
  - rights of data subjects II 3 47
  - scope of application II 3 17
  - security of processing II 3 57
  - significance II 3 42
  - technical and organisational measures II 3 48
  - TOM II 3 50
  - training data II 3 46
  - transparency and information obligations II 3 44
- Generative AI** I 2 7; I 4 16
  - image and text generation I 4 13
  - strategy for the use I 4 45
- Generative AI systems**
  - distinction to personal reference II 3 11
- German Data Ethics Commission** II 1 52
- German Federal Constitutional Court** II 1 85
- German federate states' data protection laws** II 3 71

**GitHub** I 4 12

**GPAI model** I 2 7; I 4 1, 26; II 1 16

- AI Office III 1 44
- as a product I 4 31
- fines III 3 11
- GPAI system III 1 45
- image and text generation I 4 13
- risk classification II 1 54
- special rules III 3 11
- TDM exception II 3 121

**GPAI-Model** I 2 8

**GreenData4All** II 3 103

**Guidelines** II 1 139, 559; II 3 69

**Hallucinations** I 4 10

**Harmonisation legislation** II 1 127, 271

**Harmonised standards** II 1 525, 530, 532, 534

**Health research with AI** II 1 563

- complexity of legal requirements II 1 563

**Health sector** I 4 33

**High Level Expert Group on AI** III 1 30

**High-risk AI system** II 1 125, 152, 247

- administrative dogmatics II 1 135
- analysis of decision-making patterns II 1 134
- authorised representative II 1 397
- basic private and public services and benefits II 1 222
- categorisation by Annex I II 1 155
- change of provider II 1 140
- classification II 1 126, 128, 162
- completed human activity II 1 133
- cooperation with competent authorities II 1 406
- cooperation with competent national authorities II 1 415
- data protection impact assessment II 1 142
- deployer II 1 142
- design of AI systems II 1 302
- documentation II 1 293
- documentation and registration obligation of providers II 1 141
- documentation obligation II 1 142
- exceptions II 1 129, 218
- exemption from the high-risk classification II 1 137
- FOSS-AI system II 1 32
- general obligations of providers II 1 366
- grandfathering provisions I 4 64
- human oversight II 1 354
- improvement of a result of a previously completed human activity II 1 132
- independence of human oversight II 1 348
- indexing, searching, text and language processing II 1 135
- individual case no risk II 1 129
- interference with the business II 1 347

- narrow procedural task II 1 131
- not unacceptable risk II 1 125
- obligations from making available on the market II 1 412
- obligations from placing on the market II 1 403
- obligations of deployers II 1 416
- obligations of distributors II 1 409
- obligations of importer II 1 399
- obligations of providers II 1 365
- operating instructions II 1 137, 335
- placing it on the market II 1 310
- post-remote biometric identification II 1 434
- preparatory tasks II 1 135
- product regulation under the New Legislative Framework II 1 160
- product regulation under the old legal framework II 1 157
- product safety law II 1 156
- prohibited behaviour by students II 1 181
- public support and services II 1 223
- put into service II 1 310
- regulation of exceptions II 1 221
- relationship between exemption and the change of provider II 1 140
- retention of the logs II 1 378
- retroactive exceptions II 1 129
- right of amendment by the Commission II 1 143
- safety of financial livelihood II 1 222
- serious incidents III 1 30
- specific measures II 2 10
- start button II 1 132
- stop button II 1 132
- systemic risk II 1 354
- test II 1 289
- transparency II 1 332
- transparency in the use II 1 330
- vulnerable persons II 1 290
- way out of the obligations II 1 129

**High-risk classification** II 1 177

**Human capital management** II 1 218

**Human Capital Management-Systems (HCM)** I 4 56

**Human decision** II 1 213

**Human oversight** II 1 339, 354

- functioning and risks II 1 343

**Humane decision-making in the area of justice** II 1 254

**Identifying and inferring emotions** II 1 90

**Images**

- copyright II 3 131

**Implementation of the AI Act**

- laws II 3 172

**Implementation of RBI through national law** II 1 118

**Implementation of the AI Act**

- collective agreements II 3 173
- legal scope for regulation II 3 179
- level of protection II 3 178
- more favourable regulation II 3 174
- multiple objectives II 3 175
- regulatory instruments II 3 172

**Implementing acts of the Commission II 1 548****Importer II 1 21**

- inspection obligations II 1 400

**Influence of automated preliminary decisions II 1 213****Influence to working conditions II 1 215****Influencing of behavior II 1 235****Influencing of consciousness II 1 235****Information obligation for employers II 1 429****Information Security Management Systems (ISMS) II 1 278; II 3 58****Information to employers**

- transparency and provision II 1 329

**Infrastructure II 1 173****Input II 3 123; II 2 27****Input data II 3 6****Instruction error III 2 22****Instructions for use III 2 11 f.****Intensity of interference II 1 91****Internal company guidelines II 3 70****Internal risk distribution III 2 37****Internet of Things (IoT) II 3 81****Intervention threshold II 1 85****Intimidation effects II 1 81****Job interview II 3 77****Joint liability III 2 37****Judicial authority II 1 249****Judicial independence II 1 327****Knowledgeable persons II 1 309****Labour law II 3 155**

- employees II 3 167
- opening clause II 3 155, 165
- regulatory power of collective bargaining parties II 3 168
- solo self-employed persons II 3 167

**Language model I 2 7****Large language model I 4 1****Law enforcement III 1 24**

- digital evidence I 4 38

**Law enforcement purposes II 3 77****Legacy systems I 4 61****Legal advice I 4 28****Legal consultation I 4 24****Legal obligation to impart measures of AI literacy II 1 55****Legal protection**

- individual rights II 1 71

**Legal remedies III 1 56**

- right to explanation of the individual decision-making III 1 58
- right to lodge a complaint III 1 57

**Legal scope for regulation II 3 179**

- high-risk AI system II 3 180

**Legal Tech I 3 1; I 4 23; II 1 257****Legal tech in the private sector II 1 257****Levels of autonomy II 1 339****Liability II 1 553; III 2 8, 24**

- contractual liability III 2 7
- direct liability for interference III 2 35
- duty to protect III 2 24
- manufacturer III 2 17
- provider III 2 33
- pure information III 2 23
- strict liability III 2 8
- supplier III 2 17
- violation of personal rights III 2 32

**Licence II 3 112****Lie detectors II 1 232****Life and health insurance II 1 229****LLMoin I 4 48****Local storage objects II 3 80****Location-based prediction system II 1 79****Logging function**

- for biometric remote identification systems II 1 325

**Luminous I 4 48****Machine Learning I 2 6****Machine-assisted II 1 14****Machine-readable reservation of rights II 3 116****Management systems for dealing with risks II 1 278****Manufacturing defect III 2 22****Market surveillance authorities III 1 31**

- investigative powers III 1 32
- review of the classification of the system III 1 40
- special supervisory powers of investigation III 1 33
- system of assigning powers III 1 31
- training, validation and test data sets III 1 34

**Market Surveillance Regulation III 2 12****Marketplace principle II 1 25****Material distortion of behaviour II 1 58****Material scope of application II 1 10****Max-Planck-Institute**

- study for research on crime, security and law II 1 82

- Meta Platforms Ireland Limited (Meta)** III 4 3
- Metrics for measurement** II 1 358
- Migration** II 1 242, 244
- Military** II 1 39
- Minimum information in the technical documentation** II 1 317
- Model evasions** II 1 359
- Models** II 1 359
- Monitoring obligations** II 1 425
- Moral rights of artists** III 2 31
- Motion pictures** II 3 130
- Multimodal AI system** I 4 63
  
- National authorities** III 1 16 ff., 43; III 3 3
  - guidance and advice III 1 29
- National regulation** II 2 1
- National Regulatory Sandbox Act** II 1 562
- Negligence**
  - contributory III 2 37
- Neural Network** I 2 6
- New Product Liability Directive** III 2 20
- NIST** II 1 360
- Notification procedure** III 1 51
- Notified bodies** III 1 51
- Notifying authority** III 1 20
  
- Obligated parties** II 1 19
- Obligation to retain automatically generated logs** II 1 428
- Obligations in dealing with high-risk AI systems** II 1 364
- Obligations of deployers**
  - cooperation with competent national authorities II 1 441
  - duty to provide information to natural persons II 1 440
  - in connection with use II 1 417
- Obligations of the Member States** III 1 25
- Obligations under the AI Act** II 1 273
- OLGA** I 3 1
- On-premise implementations** II 3 15
- Open source** I 4 16, 21; II 1 29
- Open source AI components** II 1 30
- Open systems** II 3 70
- Opening clause** II 1 44
- Operator** II 1 50
  - violation of personal rights III 2 32 f.
- Operator liability** III 2 8
- Originality** II 3 129
- Output** III 2 28
  
- Palantir** II 1 85
- Participation and information rights** II 3 191
- Participation rights of works council** II 3 196
  
- Particularly serious criminal offences** II 1 236
- Penalties and other enforcement measures** II 2 7
- Penetration of processing with AI** II 3 68
- People analytics** I 4 58
- Personal characteristics** II 1 69
- Personal data in AI regulatory sandbox**
  - further processing for different purpose II 1 550
- Personal reference** II 3 7
- Personal rights** II 3 136
  - AI-generated content II 3 138
  - violation II 3 138
- Personal scope of application** II 1 18, 24
- Personal training data** II 3 8
- Personnel selection** II 1 212
- Phonogram** II 3 132
- Platform Directive** II 3 155, 182, 192
  - monitoring systems II 3 192
- Platform Work Directive** II 3 167
- Police database**
  - independent suggestions for processing and linking police data II 1 84
  - organisation and structure II 1 83
- Police laws** II 1 234
- Positive catalogue** II 1 128
- Practice of the supervisory authorities** III 4 3
- Predictive policing** II 1 76, 80
  - risks II 1 81
- Preliminary decisions** II 1 254
- Preparedness Framework** II 1 174
- Press publication** II 3 133
- Presumption of causality** III 2 16
- Presumption of conformity** II 1 534
- Private devices** II 1 47
- Privileged promotion of innovation** I 4 16
- Probability statements** II 1 92
- Processing prohibition Art. 9 para. 1 GDPR** II 1 35
- Proctoring** II 1 181
- Producer liability** III 2 21
  - breach of duty III 2 22
  - burden of proof III 2 22
- Product** II 1 45
- Product Liability Act** III 2 19
- Product monitoring obligation** III 2 21
- Product safety** II 1 48
- Product Safety Act**
  - new III 2 25
- Product safety law** I 4 65; III 2 25
- Profiling** II 1 170
- Profiling Art. 3 para. 4 EU Directive 2016/680** II 1 77
- Profiling of data subjects** II 1 130
- Prohibition with reservation of authorisation**
  - GDPR II 3 19



- Promotion of innovation** II 1 559
  - SME II 1 559
  - start-ups II 1 559
- Prompts** II 3 123; III 2 27
- Prosecution of criminal offences** II 1 232 f.
- Prosecutorial decision-making process** I 4 40
- Protected legal interests** II 1 17
- Protection of databases sui generis** II 3 119
- Protection of fundamental rights** III 1 43
- Protection of privacy in terminal equipment** II 3 76, 78
- Protective law** III 2 11
- Provided** II 1 31
- Provider role** II 1 196
- Pseudonymisation** II 1 250
- Public administration** I 4 47
- Public sector bodies** II 3 88
- Public Service Information Directive** II 3 162
- Put into service**
  - necessary information II 1 381
- Qualification Directive** II 1 245
- Quality management** II 1 368
  - minimum contents II 1 369
- Quality management system** II 1 292
- Quality of data sets** II 1 536
- Quality of the database** II 3 142
- Real-time remote biometric identification systems** II 2 6
- Real-time remote identification** II 1 104
- Recognisability of attacks** II 1 357
- Reconstruction of personal data** II 3 10
- Record-keeping obligations** II 1 319
- Recruitment and selection** II 1 211
- Referendum** II 1 259
- Registration** II 1 430
- Regularly sandbox**
  - overarching standards II 1 562
- Regulatory sandbox** II 1 540; II 3 186
  - experimentation clause check II 1 562
  - legal basis II 1 562
  - one-stop shop for real world laboratories (OSS) II 1 562
- Reinforcement Learning** I 2 6
- Reinforcement Learning from Human Feedback (RLHF)** I 4 9
- Related property rights**
  - AI output II 3 130
- Relationship of the special transparency obligations to the Digital Services Act** II 1 475
- Requirements of the GDPR** II 3 50
- Research** II 1 549
- Research privilege** II 1 37
- Research system** II 1 36
- Reservation of rights** II 3 116
  - text and data mining II 3 116
- Resilience of Critical Entities Directive** II 1 172
- Responsibility** II 3 12
  - training and input data II 3 13
- Responsibility under data protection law** II 3 12
- Right of amendment by the Commission of Annex III** II 1 146
- Right to lodge a complaint**
  - market surveillance authority III 1 57
- Risk concepts** II 1 142
- Risk management frameworks** II 1 280
- Risk management measures** II 1 282, 287 f.
- Risk management system** II 1 277, 281, 292, 536
  - dynamic component II 1 283
  - intended purpose II 1 284
  - restriction of the risk assessment II 1 285
  - systematic review and updating II 1 282
- Risk mitigation measures** III 2 36
- Risk of circumvention** I 4 61
- Risk to rights and freedoms of natural persons** II 3 33
- Risk-based approach** II 1 51
- Risk-based regulatory concept** II 1 51
- RLHF** I 4 9
- Robotic** I 3 2
- Safety requirements of technical robustness** II 1 357
- Sanctions** III 3 1, 14
- Sandboxing options** II 3 186
- Schematic structured decisions** I 4 40
- School** I 4 44; II 1 199
  - grading suggestions II 1 199
- School administration** I 4 45
- Schufa decision of the ECJ** II 1 201
- Schufa judgement of the ECJ** II 3 40
- Schufa score** II 3 73
- Scope of application** II 1 7
  - AI Act II 2 3
  - Art. 111 II 1 50
  - GDPR II 3 17
  - material II 1 10
  - personal II 1 18, 24
  - territorial II 1 25
- Secrecy of telecommunications** II 3 76
- Security of automated processing** II 3 75
- Self-employment** II 1 207
- Service description** II 1 198
- Simple AI system** II 1 477
- Simple algorithmic system** II 1 136
- Small and medium sized enterprises** III 3 10
- Smart Contracts** I 4 23
- Social behaviour** II 1 69

- Social media**
  - disruptive potential II 2 17
- Social scoring** II 1 69 f., 224
- Sociology** II 1 307
- Software** II 1 14
- Source code** III 1 35
- Special categories of personal data** II 3 33
- Special transparency obligations** II 1 457
- Spheres of responsibility** II 3 164
- Sports** I 4 33
- Standardisation bodies** II 1 528
- Standardisation documents** II 1 534
- Standardisation in the AI Act** II 1 530
- Standards** II 3 69
- Start button** II 1 350
- State liability law** I 4 44
- State of the art** II 1 270
- State support with financial and material resources** II 1 223
- Strategic personnel deployment** II 1 218
- Subliminal influence** II 1 58
- Substantial change** I 4 66
- Supervised Learning** I 2 6
- Supervision** II 1 548
- Supervisory measures** III 1 36
  - Market Surveillance Regulation III 1 36
- Switch to the operator role** I 4 32
- Symbolic AI** I 2 2
- Symptom checker** I 4 34
- Systemic risk** II 1 174
- Systems**
  - placed on the market II 1 49
  - put into service II 1 49
- Taking corrective actions** II 1 381
- Talent management** I 4 28
- Tax consultation** I 4 24
- Teacher** II 1 196
- Technical and organisational measures**
  - fault security plans II 1 359
  - IT security requirements II 1 361
  - state of the art II 1 360
- Technical and organisational measures to control risks** II 3 49
- Technical design specifications** II 1 361
- Technical documentation** II 1 309
- Technical guidelines** II 3 69
- Telecommunications and Digital Services Data Protection Act (TTDSG)** II 3 76
- Telemedicine** I 4 34
- Temperature of the AI system** II 3 143
- Terms of use** III 2 38
- Territorial scope of application** II 1 25
- Test data set** II 1 301
- Testing data** II 3 5
- Testing plan** II 1 555
- Testing under real conditions** II 1 554
- Text and data mining** II 3 113
  - commercial purposes II 3 115
  - copyright II 3 113
  - databases II 3 119
  - generative GPAI II 3 121
  - lawful access II 3 118
  - non-commercial purposes II 3 114
  - scientific purposes II 3 113
- Thinking tools** II 1 184
- Three-stage process (provider – user – human oversight)** II 1 345
- TikTok Technology Limited (TikTok)** III 4 3
- Tort law** III 2 9
- Trace approach** II 1 85
- Traffic management** I 4 50
- Training** II 1 192
- Training data** II 3 5
- Training data set**
  - manipulation II 1 359
- Training data sets** II 1 301
- Translation** III 2 29
- Transparency** II 1 93
- Triage situation** II 1 231
- Trust in state structures** II 1 81
- Trustworthy AI** II 1 17
- Two-person constellations** II 3 42
- Two-pillar-model** II 2 18
- Typical conditions of use** II 1 304
- Unfavourable treatment** II 1 70
- Union bodies** III 3 11
  - fines III 3 12
- University** II 1 186
- University management** II 1 194
- Unjustified negative consequences** II 1 70
- Use Cases** I 4 11
- Use of AI**
  - below the threshold of the decision substitute II 1 236
  - gathering evidence II 1 237
  - HR sector I 4 59
  - prosecution of criminal offences II 1 236
  - substitute for a decision II 1 241
  - supportive use of AI II 1 236
- Use of RBI** II 1 102
  - annual report of market surveillance and data protection authorities II 1 120
  - crime investigations II 1 107
  - defence against serious threats II 1 106
  - fundamental rights impact assessment II 1 113
  - intervention impact assessment II 1 112
  - notification to market surveillance authority and data protection authority II 1 117
  - permitted purposes II 1 105

- registration **II 1 113**
- requirements **II 1 110**
- search for missing persons **II 1 105**
- search for victims of criminal offences **II 1 105**
- situation impact assessment **II 1 111**

**User liability III 2 8**

**Validation data II 3 5**

**Validation data sets II 1 301**

**Verification when using biometric remote identification systems II 1 351**

**Very large online platforms II 3 108**

**Victim of criminal offences II 1 232**

**Violation of personal rights**

- liability **III 2 32**
- operator of the AI system **III 2 32 f.**

**Voting behaviour of natural persons II 1 259**

**Weak AI I 2 8**

**Whistleblower Directive III 1 59**

**Work output enhancement I 4 55**

**Worker's management II 1 202 f., 208, 213, 219**