

Artificial Intelligence Act (AI Act)

Contents

1.	Description	8
2.	Scope	9
3.	Key Information	9
4.	Penalties	10
5.	Roles	11
5.1	Provider	11
5.2	Deployer	12
5.3	Importer	12
5.4	Distributor	12
5.5	Authorised representative	12
6.	Policy Coverage	13
6.1	Prohibited AI practices	13
6.1.1	Systems using subliminal or purposefully manipulating or deceptive techniques	13
6.1.2	Systems exploiting vulnerabilities	13
6.1.3	Biometric categorisation	14
6.1.4	Social scoring systems	14
6.1.5	“Real-time” remote biometric identification systems	14
6.1.6	Predictive policing systems	15
6.1.7	Creating or expanding facial recognition databases through untargeted scraping of facial images	15
6.1.8	Emotion recognition systems	16
6.1.9	Prohibitions coming from infringements of other Union law	16
6.2	High-risk	16

6.2.1 Machinery and related components	17
6.2.2 Toys	18
6.2.3 Recreational craft, personal watercraft, and related components	18
6.2.4 Lifts and safety components for lifts	19
6.2.5 Equipment and protective systems intended for use in potentially explosive atmospheres	20
6.2.6 Radio equipment	20
6.2.7 Pressure equipment	21
6.2.8 Cableway installations	21
6.2.9 Personal protective equipment	21
6.2.10 Appliances burning gaseous fuels and related safety devices	22
6.2.11 Medical devices	22
6.2.12 In vitro diagnostic medical devices	23
6.2.13 Civil aviation security	24
6.2.14 Two- or three-wheel vehicles and quadricycles	24
6.2.15 Agricultural and forestry vehicles	25
6.2.16 Marine equipment	25
6.2.17 Rail systems	25
6.2.18 Motor vehicles and their trailers	26
6.2.19 Products, parts and equipment for remote control of an aircraft	27
6.2.20 Biometrics permitted under Union or national law	28
6.2.21 Critical infrastructure	29
6.2.22 Education and vocational training	29
6.2.23 Employment, workers management and access to self-employment	30
6.2.24 Essential private services and essential public services and benefits	30
6.2.25 Law enforcement, permitted under Union or national law	31

6.2.26 Migration, asylum and border control management, permitted under Union or national law	31
6.2.27 Administration of justice and democratic processes	32
6.3 General purpose AI	33
6.3.1 General-purpose AI models	33
6.3.2 General-purpose AI system	33
6.4 General purpose AI models with systemic risk	34
6.4.1 General-purpose AI models with systemic risk	34
6.5 Transparency risk	35
6.5.1 Systems interacting with natural persons	35
6.5.2 Systems generating synthetic audio, image, video or text content	35
6.5.3 Emotion recognition and biometric categorisation systems	35
6.5.4 Systems generating or manipulating content (deepfakes)	36
6.6 Minimal or no risk	36
6.6.1 Minimal or no risk AI system	36
6.7 Open source	37
6.7.1 AI systems under free and open source license	37
7. Policy Requirements	37
7.1 Exemption from high-risk system classification	37
7.1.1 Assessment of exemption from high-risk classification	38
7.1.2 Registration to EU or national database	38
7.1.3 Cooperation with national competent authority	39
7.2 Risk management system	40
7.2.1 Risk management system policies and processes	40
7.2.2 Risk identification and evaluation process	40
7.2.3 Risk management measures adoption	41

7.2.4 Risk testing procedures	42
7.2.5 Assessment of impacts on children and vulnerable groups of people	42
7.2.6 Integrated risk management under relevant sectorial Union law	42
7.3 Data and data governance	43
7.3.1 Data governance and management practices	43
7.3.2 Dataset representativeness and completeness	44
7.3.3 Dataset relevancy and applicability	44
7.3.4 Special categories of personal data	44
7.4 Technical documentation	45
7.4.1 General description of the AI system	46
7.4.2 Description of AI system elements and its development process	46
7.4.3 Information on monitoring, functioning, and control of the AI system	47
7.4.4 Risk management	48
7.4.5 Change management	48
7.4.6 Harmonised standards	48
7.4.7 EU declaration of conformity	49
7.4.8 Post-market monitoring plan	49
7.5 Record-keeping	49
7.5.1 Logging for system lifecycle and risk monitoring	50
7.5.2 Logging requirements for remote biometric identification systems	50
7.6 Transparency and provision of information to deployers (Instructions for use)	51
7.6.1 Provider contact details	51
7.6.2 Characteristics, capabilities, and limitations of performance of the system	51
7.6.3 Pre-determined changes	52
7.6.4 Human oversight measures	52

7.6.5 Computational and hardware resources, expected lifetime and necessary maintenance measures	53
7.6.6 Log management	53
7.7 Human oversight	53
7.7.1 Effective oversight	54
7.7.2 Human oversight measures	54
7.7.3 Human oversight measures for biometric identification systems	55
7.8 Accuracy, robustness and cybersecurity	55
7.8.1 Performance and accuracy assurance	56
7.8.2 Resilience and robustness	56
7.8.3 Cybersecurity resilience	57
7.9 Quality management system	57
7.9.1 Strategy for compliance	58
7.9.2 Design, control, and verification procedures	58
7.9.3 Development and quality assurance procedures	58
7.9.4 Examination, testing, and validation procedures	58
7.9.5 Technical specifications and compliance assurances	59
7.9.6 Data management systems and procedures	59
7.9.7 Risk management system	59
7.9.8 Establishment and maintenance of post-market monitoring system	60
7.9.9 Procedures for reporting serious incidents	60
7.9.10 Communication and management with regulatory authorities and relevant stakeholders	60
7.9.11 Record keeping systems and procedures	60
7.9.12 Resource management	61
7.9.13 Accountability framework	61
7.9.14 Providers subject to quality management system under sectorial Union law	61

7.9.15 Integrated quality management system - Directive 2013/36/EU	61
7.10 Conformity assessment	62
7.10.1 Presumption of conformity with certain requirements	62
7.10.2 Harmonised standards and common specifications	63
7.10.3 Conformity assessment procedure based on internal control	64
7.10.4 Conformity based on third-party assessment	65
7.10.5 Conformity assessment of high-risk AI systems in Annex II, section A	66
7.10.6 Requirement to undergo new conformity assessment	66
7.10.7 Certificate of conformity	67
7.10.8 EU declaration of conformity	67
7.10.9 CE marking of conformity	68
7.11 Obligations of providers of high-risk AI systems	69
7.11.1 Identification and contact information	70
7.11.2 Document retention	70
7.11.3 Automatically generated logs	71
7.11.4 Corrective actions and duty of information	71
7.11.5 Cooperation with authorities	72
7.11.6 Accessibility requirements	72
7.11.7 Registration to EU or national database	73
7.11.8 Reporting of serious incidents	74
7.12 Post-market monitoring	75
7.12.1 Post-market monitoring plan	75
7.13 Enforcement by market surveillance authorities	76
7.13.1 Application of Regulation (EU) 2019/1020 on Market Surveillance and Compliance of Products	76
7.13.2 Access to high-risk AI system documentation, data, and source code	77

7.13.3 Monitoring and information access for general-purpose AI systems	78
7.13.4 Supervision of AI system testing in real-world conditions	79
7.13.5 Access of authorities protecting fundamental rights to high-risk AI system documentation	79
7.13.6 Non-compliant AI systems presenting a risk at the national level	80
7.13.7 Compliant AI systems presenting risk at the national level	81
7.13.8 AI systems classified as not high-risk AI systems	81
7.13.9 Formal non-compliance	82
7.14 Appointment and obligations of authorised representative	83
7.14.1 Appointment and mandate of the authorised representative	83
7.14.2 Tasks of the authorised representative	83
7.14.3 Termination of mandate by authorised representative	84
7.15 Importer obligations	85
7.15.1 Pre-market placement obligations	85
7.15.2 Identification and contact information	86
7.15.3 Compliance assurance	86
7.15.4 Document retention	86
7.15.5 Information provision and collaboration	87
7.15.6 Cooperation with national authorities	87
7.16 Distributor obligations	87
7.16.1 Pre-market verification	88
7.16.2 Compliance assurance	88
7.16.3 Post-market corrective actions	89
7.16.4 Information provision and collaboration	89
7.16.5 Cooperation with national authorities	89
7.17 AI value chain responsibilities and provider obligation transfer	90

7.17.1 Transfer of provider obligations	90
7.17.2 Provider obligations of manufacturers of safety components of products	91
7.17.3 Supplier obligations	91
7.18 Deployer obligations	92
7.18.1 Measures to comply with the instructions of use	92
7.18.2 Implement human oversight	93
7.18.3 Ensure input data relevance and representativeness	93
7.18.4 Monitoring and reporting obligations	93
7.18.5 Record-keeping	94
7.18.6 Workplace deployment notification	95
7.18.7 Registration to EU or national database by public authorities or persons acting on their behalf	95
7.18.8 Compliance with data protection impact assessment obligations	96
7.18.9 Judicial authorisation for exempted use of post-remote biometric identification	96
7.18.10 AI decision transparency disclosure	96
7.18.11 Cooperation with national authorities	97
7.18.2 Fundamental rights impact assessment	97
7.19 Transparency obligations of certain AI systems	98
7.19.1 AI interaction transparency	99
7.19.2 Synthetic content disclosure and marking requirement	99
7.19.3 Emotion recognition and biometric categorisation transparency	100
7.19.4 Disclosures of AI-generated deep fake content	100
7.19.5 Disclosure of AI-generated public interest text	101
7.20 Obligations for general purpose AI models	101
7.20.1 GPAI technical documentation	102
7.20.2 Downstream provider transparency and instructions of use	103

7.20.3 Compliance with copyright law	104
7.20.4 Documentation and publishing of training data	104
7.20.5 Cooperation with authorities	105
7.21 Obligations for general purpose models with systemic risk	105
7.21.1 Supplementary technical documentation	105
7.21.2 Standardised model evaluation and adversarial testing	106
7.21.3 Risk assessment and mitigation	106
7.21.4 Incident and corrective measure tracking, documenting, and reporting	107
7.21.5 Cybersecurity protection	107
7.22 Appointment and obligations of authorised representatives for GPAI	107
7.22.1 Appointment and mandate of the GPAI authorised representative	108
7.22.2 Tasks of the GPAI authorised representative	108
7.22.3 Termination of mandate by GPAI authorised representative	109
7.23.1 Codes of conduct	109
7.23.2 Voluntary codes of conduct	110