



EU AI ACT 2024/1689

*Controls Checklist (Draft)*

**EU AI Act**

**EU 2024/1689**

***Controls Checklist***

Version: 0.1 (Draft)

Last Update: 18 Jul, 2024

# TABLE OF CONTENT

## Contents

TABLE OF CONTENT .....	2
DISCLAIMER .....	7
INTRODUCTION .....	8
CHAPTER II PROHIBITED AI PRACTICES, ARTICLE 5 PROHIBITED AI PRACTICES.....	9
<i>Prohibited AI Practices</i> .....	9
AIAct-001: Avoid Subliminal and Manipulative AI Techniques .....	9
AIAct-002: Prevent Exploitation of Vulnerabilities .....	11
AIAct-003: Prohibit Social Scoring Systems.....	12
AIAct-004: Restrict Risk Assessments Based Solely on Profiling .....	14
AIAct-005: Prohibit Untargeted Facial Recognition Database Creation .....	15
AIAct-006: Restrict Emotion Recognition in Workplaces and Education.....	16
AIAct-007: Prohibit Biometric Categorization Based on Sensitive Attributes .....	17
AIAct-008: Restrict Real-Time Remote Biometric Identification Systems in Public Spaces .....	18
AIAct-009: Ensure Proportionality and Safeguards for Real-Time Biometric Identification Systems.....	20
AIAct-010: Obtain Prior Authorization for Real-Time Biometric Identification Systems .....	22
AIAct-011: Notify Market Surveillance and Data Protection Authorities .....	24
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 1 CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK, ARTICLE 6	
CLASSIFICATION RULES FOR HIGH-RISK AI SYSTEMS .....	25
<i>High-Risk AI System Classification</i> .....	25
AIAct-012: Identify High-Risk AI Systems Based on Safety Component or Product .....	25
AIAct-013: Identify High-Risk AI Systems Listed in Annex III.....	27
AIAct-014: Assess Risk of Harm and Influence on Decision Making .....	28
AIAct-015: Document Risk Assessment for Non-High-Risk AI Systems .....	30
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 REQUIREMENTS FOR HIGH-RISK AI SYSTEMS, ARTICLE 8	
COMPLIANCE WITH THE REQUIREMENTS .....	31
<i>Compliance with Requirements for High-Risk AI Systems</i> .....	31
AIAct-016: Compliance with High-Risk AI System Requirements .....	31
AIAct-017: Compliance with Union Harmonisation Legislation.....	33
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 REQUIREMENTS FOR HIGH-RISK AI SYSTEMS, ARTICLE 9 RISK	
MANAGEMENT SYSTEM .....	34
<i>Risk Management System for High-Risk AI Systems</i> .....	34
AIAct-018: Establish and Maintain Risk Management System for High-Risk AI Systems.....	34
AIAct-019: Implement Continuous Iterative Risk Management Process .....	35
AIAct-020: Identify and Analyze Known and Foreseeable Risks.....	36
AIAct-021: Estimate and Evaluate Risks under Intended Use and Misuse .....	37
AIAct-022: Evaluate Risks Based on Post-Market Monitoring Data .....	38
AIAct-023: Adopt Appropriate Risk Management Measures .....	39
AIAct-024: Focus on Mitigable or Eliminate Risks.....	40
AIAct-025: Consider Combined Effects of Requirements .....	41

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

AIAct-026: Ensure Acceptable Residual Risk .....	42
AIAct-027: Eliminate or Reduce Risks Through Design and Development .....	43
AIAct-028: Implement Mitigation and Control Measures for Unmitigable Risks .....	44
AIAct-029: Provide Information and Training to Deployers .....	45
AIAct-030: Test High-Risk AI Systems for Risk Management .....	46
AIAct-031: Consider Real-World Testing .....	47
AIAct-032: Test Throughout Development and Before Market Release .....	48
AIAct-033: Consider Impact on Vulnerable Groups .....	49
AIAct-034: Integrate Risk Management with Other Legal Requirements .....	50
<b>CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 REQUIREMENTS FOR HIGH-RISK AI SYSTEMS, ARTICLE 10</b>	
<b>DATA AND DATA GOVERNANCE .....</b>	<b>51</b>
<i>Data and Data Governance for High-Risk AI Systems</i> .....	51
AIAct-035: Ensure Data Set Quality for High-Risk AI System Development .....	51
AIAct-036: Implement Data Governance and Management Practices for High-Risk AI Systems .....	52
AIAct-037: Document and Review Design Choices for High-Risk AI Systems .....	53
AIAct-038: Document Data Collection Processes and Origin for High-Risk AI Systems .....	54
AIAct-039: Document Data Preparation Processing Operations for High-Risk AI Systems .....	55
AIAct-040: Document and Review Assumptions about Data for High-Risk AI Systems .....	56
AIAct-041: Assess Data Set Availability, Quantity, and Suitability for High-Risk AI Systems .....	57
AIAct-042: Examine Data Sets for Potential Biases in High-Risk AI Systems .....	58
AIAct-043: Implement Measures to Detect, Prevent, and Mitigate Biases in High-Risk AI Systems .....	59
AIAct-044: Identify and Address Data Gaps and Shortcomings for High-Risk AI Systems .....	60
AIAct-045: Ensure Data Set Relevance, Representativeness, Accuracy, and Completeness for High-Risk AI Systems .....	61
AIAct-046: Consider Geographical, Contextual, Behavioral, and Functional Settings for High-Risk AI Systems .....	62
AIAct-047: Process Special Categories of Personal Data for Bias Detection and Correction in High-Risk AI Systems .....	63
AIAct-048: Demonstrate Necessity of Special Categories of Personal Data for Bias Detection and Correction .....	64
AIAct-049: Implement Technical Limitations and Privacy-Preserving Measures for Special Categories of Personal Data .....	65
AIAct-050: Secure and Protect Special Categories of Personal Data with Strict Controls and Access Documentation .....	66
AIAct-051: Restrict Transmission, Transfer, and Access of Special Categories of Personal Data .....	67
AIAct-052: Delete Special Categories of Personal Data After Bias Correction or Retention Period .....	68
AIAct-053: Document Rationale for Processing Special Categories of Personal Data for Bias Detection and Correction .....	69
AIAct-054: Apply Data Governance and Management Practices to Testing Data Sets for High-Risk AI Systems Without Training .....	70
<b>CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 REQUIREMENTS FOR HIGH-RISK AI SYSTEMS, ARTICLE 11</b>	
<b>TECHNICAL DOCUMENTATION .....</b>	<b>71</b>
<i>Technical Documentation Requirements</i> .....	71
AIAct-055: Develop and Maintain Technical Documentation for High-Risk AI Systems .....	71
AIAct-056: Ensure Technical Documentation Demonstrates Compliance .....	72
AIAct-057: Include Required Elements in Technical Documentation .....	73
AIAct-058: Simplified Technical Documentation for SMEs .....	74
AIAct-059: Consolidated Technical Documentation for Combined Products .....	75
<b>CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 REQUIREMENTS FOR HIGH-RISK AI SYSTEMS, ARTICLE 12</b>	
<b>RECORD-KEEPING .....</b>	<b>76</b>
<i>Record-keeping for High-Risk AI Systems</i> .....	76
AIAct-060: Implement Logging Capabilities for High-Risk AI Systems .....	76

AIAct-061: Log Events Relevant for Traceability and Monitoring .....	77
AIAct-062: Implement Minimum Logging Requirements for Specific High-Risk AI Systems .....	78
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 REQUIREMENTS FOR HIGH-RISK AI SYSTEMS, ARTICLE 13	
TRANSPARENCY AND PROVISION OF INFORMATION TO DEPLOYERS .....	80
<i>Transparency and Provision of Information to Deployers</i> .....	80
AIAct-063: Ensure Transparency in High-Risk AI System Design and Development .....	80
AIAct-064: Provide Instructions for Use for High-Risk AI Systems .....	81
AIAct-065: Provide Provider Identity and Contact Information .....	82
AIAct-066: Document High-Risk AI System Characteristics, Capabilities, and Limitations .....	83
AIAct-067: Document Pre-Determined Changes to High-Risk AI System .....	85
AIAct-068: Document Human Oversight Measures and Technical Support for Interpretation .....	86
AIAct-069: Document Computational and Hardware Resources, Lifetime, and Maintenance Requirements .....	87
AIAct-070: Document Log Collection, Storage, and Interpretation Mechanisms .....	88
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 REQUIREMENTS FOR HIGH-RISK AI SYSTEMS, ARTICLE 14	
HUMAN OVERSIGHT .....	89
<i>Human Oversight for High-Risk AI Systems</i> .....	89
AIAct-071: Design for Human Oversight .....	89
AIAct-072: Risk Mitigation through Human Oversight .....	90
AIAct-073: Implementation of Oversight Measures .....	91
AIAct-074: Enable Effective Human Oversight .....	92
AIAct-075: Double Verification for High-Risk AI Systems .....	94
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 REQUIREMENTS FOR HIGH-RISK AI SYSTEMS, ARTICLE 15	
ACCURACY, ROBUSTNESS AND CYBERSECURITY .....	95
<i>Accuracy, Robustness, and Cybersecurity of High-Risk AI Systems</i> .....	95
AIAct-076: Ensure Accuracy, Robustness, and Cybersecurity of High-Risk AI Systems .....	95
AIAct-077: Declare Accuracy Metrics in Instructions for Use .....	96
AIAct-078: Implement Resilience Measures for High-Risk AI Systems .....	97
AIAct-079: Implement Technical Redundancy Solutions .....	98
AIAct-080: Mitigate Bias in Feedback Loops for Continuously Learning AI Systems .....	99
AIAct-081: Enhance Cybersecurity of High-Risk AI Systems .....	100
AIAct-082: Tailor Cybersecurity Solutions to Specific Risks .....	101
AIAct-083: Implement Measures to Address AI-Specific Vulnerabilities .....	102
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 OBLIGATIONS OF PROVIDERS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES, ARTICLE 16 OBLIGATIONS OF PROVIDERS OF HIGH-RISK AI SYSTEMS .....	103
<i>Obligations of Providers of High-Risk AI Systems</i> .....	103
AIAct-084: Ensure Compliance with High-Risk AI System Requirements .....	103
AIAct-085: Provide Clear Identification and Contact Information .....	104
AIAct-086: Implement a Compliant Quality Management System .....	105
AIAct-087: Maintain Required Documentation for High-Risk AI Systems .....	106
AIAct-088: Maintain Logs of High-Risk AI System Activity .....	107
AIAct-089: Conduct Conformity Assessment for High-Risk AI Systems .....	108
AIAct-090: Prepare EU Declaration of Conformity for High-Risk AI Systems .....	109
AIAct-091: Affix CE Marking to High-Risk AI Systems .....	110
AIAct-092: Comply with Registration Obligations for High-Risk AI Systems .....	111
AIAct-093: Implement Corrective Actions and Provide Information for High-Risk AI Systems .....	112
AIAct-094: Demonstrate Conformity of High-Risk AI Systems to Competent Authorities .....	113
AIAct-095: Ensure Accessibility of High-Risk AI Systems .....	114
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 OBLIGATIONS OF PROVIDERS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES, ARTICLE 17 QUALITY MANAGEMENT SYSTEM .....	115

<i>Quality Management System for High-Risk AI Systems</i> .....	115
AIAct-096: Establish a Quality Management System for High-Risk AI Systems .....	115
AIAct-097: Develop a Regulatory Compliance Strategy .....	116
AIAct-098: Implement Design Control and Verification Procedures .....	117
AIAct-099: Establish Development, Quality Control, and Assurance Procedures .....	118
AIAct-100: Implement Examination, Testing, and Validation Procedures .....	119
AIAct-101: Apply Technical Specifications and Standards .....	120
AIAct-102: Implement Data Management Systems and Procedures .....	121
AIAct-103: Integrate Risk Management System .....	122
AIAct-104: Establish and Maintain a Post-Market Monitoring System .....	123
AIAct-105: Implement Serious Incident Reporting Procedures .....	124
AIAct-106: Establish Communication Procedures .....	125
AIAct-107: Implement Record-Keeping Systems and Procedures .....	126
AIAct-108: Implement Resource Management and Security-of-Supply Measures .....	127
AIAct-109: Establish an Accountability Framework .....	128
AIAct-110: Proportionate Implementation of Quality Management System .....	129
AIAct-111: Integrate Quality Management System with Sectoral Union Law .....	130
AIAct-112: Fulfill Quality Management System Obligations for Financial Institutions .....	131
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 OBLIGATIONS OF PROVIDERS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES, ARTICLE 18 DOCUMENTATION KEEPING .....	132
<i>Documentation Keeping</i> .....	132
AIAct-113: Maintain Documentation for High-Risk AI Systems .....	132
AIAct-114: Maintain Technical Documentation for Financial Institutions .....	134
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 OBLIGATIONS OF PROVIDERS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES, ARTICLE 19 AUTOMATICALLY GENERATED LOGS .....	135
<i>Automatically Generated Logs</i> .....	135
AIAct-115: Maintain Automatically Generated Logs .....	135
AIAct-116: Maintain Logs for Financial Institutions .....	137
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 OBLIGATIONS OF PROVIDERS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES, ARTICLE 21 COOPERATION WITH COMPETENT AUTHORITIES .....	138
<i>Cooperation with Competent Authorities</i> .....	138
AIAct-119: Provide Information and Documentation to Competent Authorities .....	138
AIAct-120: Provide Access to AI System Logs .....	140
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 OBLIGATIONS OF PROVIDERS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES, ARTICLE 25 RESPONSIBILITIES ALONG THE AI VALUE CHAIN .....	141
<i>Responsibilities along the AI value chain</i> .....	141
AIAct-146: Compliance with Provider Obligations for High-Risk AI Systems .....	141
AIAct-147: Brand Association with High-Risk AI Systems .....	142
AIAct-148: Substantial Modification of High-Risk AI Systems .....	143
AIAct-149: Modification of Intended Purpose for High-Risk AI Systems .....	144
AIAct-150: Cooperation and Information Sharing for High-Risk AI Systems .....	145
AIAct-151: Product Manufacturer Responsibility for High-Risk AI Systems .....	146
AIAct-152: Brand Association with High-Risk AI Systems in Products .....	147
AIAct-153: Brand Association with High-Risk AI Systems in Products (Post-Market) .....	148
AIAct-154: Collaboration Agreements for High-Risk AI Systems .....	149
AIAct-155: Protection of Intellectual Property and Confidential Information .....	150
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 OBLIGATIONS OF PROVIDERS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES, ARTICLE 27 FUNDAMENTAL RIGHTS IMPACT ASSESSMENT FOR HIGH-RISK AI SYSTEMS .....	151

<i>Fundamental Rights Impact Assessment for High-Risk AI Systems</i> .....	151
AIAct-168: Conduct Fundamental Rights Impact Assessment .....	151
AIAct-169: Document Deployment Processes .....	153
AIAct-170: Define Deployment Timeline and Frequency .....	154
AIAct-171: Identify Affected Individuals and Groups .....	155
AIAct-172: Assess Risks of Harm .....	156
AIAct-173: Implement Human Oversight Measures .....	157
AIAct-174: Develop Risk Mitigation Strategies .....	158
AIAct-175: Maintain and Update Impact Assessment .....	159
AIAct-176: Notify Market Surveillance Authority .....	160
AIAct-177: Integrate Data Protection Impact Assessment .....	161
CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 5 STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION, ARTICLE 40 HARMONISED STANDARDS AND STANDARDISATION DELIVERABLES .....	162
<i>Harmonised Standards and Standardisation Deliverables</i> .....	162
AIAct-178: Conformity with Harmonised Standards .....	162
AIAct-179: Promote Investment and Innovation in AI .....	164
CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING AND MARKET SURVEILLANCE, SECTION 5 SUPERVISION, INVESTIGATION, ENFORCEMENT AND MONITORING IN RESPECT OF PROVIDERS OF GENERAL- PURPOSE AI MODELS, ARTICLE 93 POWER TO REQUEST MEASURES .....	165
<i>Commission Power to Request Measures</i> .....	165
AIAct-367: Compliance with Obligations in Articles 53 and 54 .....	165
AIAct-368: Implementation of Mitigation Measures for Systemic Risk .....	166
AIAct-369: Restriction, Withdrawal, or Recall of General-Purpose AI Models .....	167
CHAPTER XIII FINAL PROVISIONS, ARTICLE 111 AI SYSTEMS ALREADY PLACED ON THE MARKET OR PUT INTO SERVICE AND GENERAL-PURPOSE AI MODELS ALREADY PLACED ON THE MARKET .....	168
<i>AI Systems Already Placed on the Market</i> .....	168
AIAct-372: Compliance with Regulation for Existing AI Systems .....	168
AIAct-373: Compliance with Regulation for Existing High-Risk AI Systems .....	170
AIAct-374: Compliance with Regulation for Existing General-Purpose AI Models .....	171
<b>END OF DOCUMENT</b> .....	<b>172</b>

# DISCLAIMER

---

This document is intended exclusively for professional exchange of ideas. The information provided herein is for educational purposes only and does not constitute professional advice.

## No Warranties or Liability

This document is provided "as is" without any express or implied warranties. We assume no responsibility and disclaim all liability for any damages arising from the use of the information contained in this document.

## Seek Professional Guidance or Advice

The information contained in this document should not be applied to practical situations without consulting a qualified professional.

## Verify Before Use

This content includes AI-assisted information. It may contain errors or incorrect information. Please verify all information carefully before use.

## Reference Source:

European Union's AI Act

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

# INTRODUCTION

---

Mapping compliance requirements to controls is a lengthy and time-consuming task. This document presents a Proof of Concept (PoC) exploring the potential of Artificial Intelligence (AI) to streamline the process of analyzing compliance documents and aligning them with relevant control activities. The focus is on the EU AI Act compliance requirements, organized into distinct sections with an accompanying implementation guide.

Various AI prompts, models, and approaches were tested to evaluate the feasibility of developing an enterprise-level risk and compliance consulting service deliverable using AI technologies. This document is available for use and sharing among Governance, Risk, and Compliance (GRC) professionals to support their work. I hope this checklist can serve as reference material for GRC professionals studying EU AI Act requirements.

This is a draft version for community reference and comment. Some incorrect content is expected in this draft version.

All relevant data and resources will be accessible through the GRC Library at <https://grclibrary.com>.

For comments or feedback, please visit the GRC Library website or their LinkedIn page: <https://www.linkedin.com/company/grclibrary>.

Important Notes: No control duplication checking in this draft version

Best Regards,

Victor Tong (LinkedIn: <https://www.linkedin.com/in/vsctong>)



## CHAPTER II PROHIBITED AI PRACTICES, Article 5 Prohibited AI practices

### Prohibited AI Practices

*To prohibit certain AI practices that pose significant risks to individuals and society.*

#### AIAct-001: Avoid Subliminal and Manipulative AI Techniques

##### Control Objective:

To ensure that AI systems do not employ subliminal or manipulative techniques that could materially distort a person's behavior.

##### Implementation Guidance:

1. Conduct thorough risk assessments to identify and mitigate any potential for subliminal or manipulative techniques in AI systems.
2. Implement robust ethical guidelines and principles to guide the development and deployment of AI systems.
3. Ensure transparency and explainability in AI systems, allowing users to understand how decisions are made.
4. Provide users with clear and accessible information about the potential risks and limitations of AI systems.
5. Establish mechanisms for user feedback and complaints regarding AI systems.
6. Regularly review and update AI systems to address any emerging risks or concerns related to subliminal or manipulative techniques.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 5, Section 1(a): 'The following AI practices shall be prohibited:

- (a)  
the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or

---

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-002: Prevent Exploitation of Vulnerabilities

### Control Objective:

To ensure that AI systems do not exploit vulnerabilities of individuals based on age, disability, or social or economic situation.

### Implementation Guidance:

1. Conduct comprehensive impact assessments to identify and mitigate potential risks of exploitation based on vulnerabilities.
2. Implement safeguards to prevent AI systems from discriminating against individuals based on protected characteristics.
3. Ensure that AI systems are designed and deployed in a way that is inclusive and accessible to all individuals.
4. Provide training and awareness programs for employees involved in AI development and deployment to promote ethical considerations and sensitivity to vulnerabilities.
5. Establish mechanisms for monitoring and reporting on the potential for exploitation of vulnerabilities by AI systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 1(b): 'The following AI practices shall be prohibited:

(b)

the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-003: Prohibit Social Scoring Systems

### Control Objective:

To prevent the development and deployment of AI systems that create social scores based on personal characteristics or behavior.

### Implementation Guidance:

1. Establish clear policies and procedures prohibiting the development and use of AI systems for social scoring.
2. Conduct due diligence on any third-party AI systems to ensure they do not engage in social scoring practices.
3. Implement robust data governance practices to prevent the collection and use of data for social scoring purposes.
4. Educate employees about the ethical implications of social scoring and the importance of adhering to the prohibition.
5. Monitor and report on any potential instances of social scoring by AI systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 1(c): 'The following AI practices shall be prohibited:

(c)  
the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i)  
detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

(ii)

detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-004: Restrict Risk Assessments Based Solely on Profiling

### Control Objective:

To ensure that AI systems used for risk assessments do not rely solely on profiling or personality traits.

### Implementation Guidance:

1. Conduct thorough risk assessments to determine if AI systems used for risk assessments rely solely on profiling or personality traits.
2. Implement safeguards to ensure that AI systems used for risk assessments are based on objective and verifiable facts directly linked to criminal activity.
3. Ensure that AI systems used for risk assessments are designed to support human assessment and not replace it.
4. Provide clear and transparent information to individuals about how AI systems are used for risk assessments.
5. Establish mechanisms for individuals to challenge risk assessments made by AI systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 1(d): 'The following AI practices shall be prohibited:

(d)

the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-005: Prohibit Untargeted Facial Recognition Database Creation

### Control Objective:

To prevent the use of AI systems for creating or expanding facial recognition databases through untargeted scraping of images.

### Implementation Guidance:

1. Establish clear policies and procedures prohibiting the use of AI systems for untargeted facial recognition database creation.
2. Conduct due diligence on any third-party AI systems to ensure they do not engage in untargeted facial recognition database creation.
3. Implement robust data governance practices to prevent the collection and use of facial images for untargeted database creation.
4. Educate employees about the ethical implications of untargeted facial recognition database creation and the importance of adhering to the prohibition.
5. Monitor and report on any potential instances of untargeted facial recognition database creation by AI systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 1(e): 'The following AI practices shall be prohibited:

- (e)  
the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-006: Restrict Emotion Recognition in Workplaces and Education

### Control Objective:

To limit the use of AI systems for emotion recognition in workplaces and education institutions, except for medical or safety purposes.

### Implementation Guidance:

1. Conduct thorough risk assessments to determine if AI systems used for emotion recognition in workplaces or education institutions are necessary for medical or safety reasons.
2. Implement safeguards to ensure that AI systems used for emotion recognition are only deployed for legitimate medical or safety purposes.
3. Provide clear and transparent information to individuals about how AI systems are used for emotion recognition.
4. Establish mechanisms for individuals to challenge emotion recognition assessments made by AI systems.
5. Regularly review and update AI systems used for emotion recognition to ensure they are still necessary and proportionate to the intended purpose.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 1(f): 'The following AI practices shall be prohibited:

- (f)  
the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-007: Prohibit Biometric Categorization Based on Sensitive Attributes

### Control Objective:

To prevent the use of AI systems for biometric categorization that infers sensitive attributes like race, political opinions, or sexual orientation.

### Implementation Guidance:

1. Establish clear policies and procedures prohibiting the use of AI systems for biometric categorization based on sensitive attributes.
2. Conduct due diligence on any third-party AI systems to ensure they do not engage in biometric categorization based on sensitive attributes.
3. Implement robust data governance practices to prevent the collection and use of biometric data for categorization based on sensitive attributes.
4. Educate employees about the ethical implications of biometric categorization based on sensitive attributes and the importance of adhering to the prohibition.
5. Monitor and report on any potential instances of biometric categorization based on sensitive attributes by AI systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 1(g): 'The following AI practices shall be prohibited:

(g)

the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-008: Restrict Real-Time Remote Biometric Identification Systems in Public Spaces

### Control Objective:

To ensure that real-time remote biometric identification systems are only used in publicly accessible spaces for law enforcement purposes under strictly limited and justified circumstances.

### Implementation Guidance:

1. Conduct thorough risk assessments to determine if the use of real-time remote biometric identification systems in publicly accessible spaces is strictly necessary for one of the permitted objectives.
2. Implement safeguards to ensure that the use of real-time remote biometric identification systems is limited to the specific objectives outlined in the regulation.
3. Ensure that the use of real-time remote biometric identification systems is subject to prior authorization by a judicial or independent administrative authority.
4. Provide clear and transparent information to individuals about how real-time remote biometric identification systems are used.
5. Establish mechanisms for individuals to challenge the use of real-time remote biometric identification systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 1(h): 'The following AI practices shall be prohibited:

(h)

the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i)

the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

---

[LinkedIn post has number of pages restriction. Full version download information can be found on the last page.](#)

(ii)

the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii)

the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-009: Ensure Proportionality and Safeguards for Real-Time Biometric Identification Systems

### Control Objective:

To ensure that the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes is proportionate, necessary, and subject to appropriate safeguards.

### Implementation Guidance:

1. Conduct thorough risk assessments to determine if the use of real-time remote biometric identification systems is proportionate to the intended objective.
2. Implement safeguards to ensure that the use of real-time remote biometric identification systems is limited to the specifically targeted individual.
3. Ensure that the use of real-time remote biometric identification systems is subject to temporal, geographic, and personal limitations.
4. Conduct fundamental rights impact assessments to evaluate the potential impact of the use of real-time remote biometric identification systems on individuals' rights and freedoms.
5. Register the system in the EU database, unless there are duly justified cases of urgency.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 2: 'The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), shall be deployed for the purposes set out in that point only to confirm the identity of the specifically targeted individual, and it shall take into account the following elements:

(a)  
the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used;

(b)

the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), of this Article shall comply with necessary and proportionate safeguards and conditions in relation to the use in accordance with the national law authorising the use thereof, in particular as regards the temporal, geographic and personal limitations. The use of the 'real-time' remote biometric identification system in publicly accessible spaces shall be authorised only if the law enforcement authority has completed a fundamental rights impact assessment as provided for in Article 27 and has registered the system in the EU database according to Article 49. However, in duly justified cases of urgency, the use of such systems may be commenced without the registration in the EU database, provided that such registration is completed without undue delay.

,

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-010: Obtain Prior Authorization for Real-Time Biometric Identification Systems

### Control Objective:

To ensure that the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes is subject to prior authorization by a competent authority.

### Implementation Guidance:

1. Obtain prior authorization from a judicial or independent administrative authority before deploying real-time remote biometric identification systems in publicly accessible spaces.
2. Ensure that the authorization request is reasoned and complies with the detailed rules of national law.
3. If the authorization is rejected, immediately stop the use of the system and discard all data and outputs.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 3: 'For the purposes of paragraph 1, first subparagraph, point (h) and paragraph 2, each use for the purposes of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 5. However, in a duly justified situation of urgency, the use of such system may be commenced without an authorisation provided that such authorisation is requested without undue delay, at the latest within 24 hours. If such authorisation is rejected, the use shall be stopped with immediate effect and all the data, as well as the results and outputs of that use shall be immediately discarded and deleted.

The competent judicial authority or an independent administrative authority whose decision is binding shall grant the authorisation only where it is satisfied, on the basis of objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric

---

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

identification system concerned is necessary for, and proportionate to, achieving one of the objectives specified in paragraph 1, first subparagraph, point (h), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In deciding on the request, that authority shall take into account the elements referred to in paragraph 2. No decision that produces an adverse legal effect on a person may be taken based solely on the output of the 'real-time' remote biometric identification system.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-011: Notify Market Surveillance and Data Protection Authorities

### Control Objective:

To ensure that the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes is notified to the relevant authorities.

### Implementation Guidance:

1. Notify the relevant market surveillance authority and the national data protection authority about the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes.
2. Ensure that the notification includes the information specified in paragraph 6 and does not include sensitive operational data.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 5, Section 4: 'Without prejudice to paragraph 3, each use of a 'real-time' remote biometric identification system in publicly accessible spaces for law enforcement purposes shall be notified to the relevant market surveillance authority and the national data protection authority in accordance with the national rules referred to in paragraph 5. The notification shall, as a minimum, contain the information specified under paragraph 6 and shall not include sensitive operational data.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 1 Classification of AI systems as high-risk, Article 6 Classification rules for high-risk AI systems

### High-Risk AI System Classification

*To establish criteria for classifying AI systems as high-risk, based on their intended use and potential impact on safety, health, and fundamental rights.*

#### AIAct-012: Identify High-Risk AI Systems Based on Safety Component or Product

##### Control Objective:

To ensure that AI systems intended for use as safety components or products covered by Annex I legislation are classified as high-risk.

##### Implementation Guidance:

1. Conduct a thorough assessment of the intended use of the AI system to determine if it is intended to be used as a safety component of a product or if it is itself a product covered by the Union harmonisation legislation listed in Annex I.
2. Verify if the product or AI system is required to undergo a third-party conformity assessment pursuant to the Union harmonisation legislation listed in Annex I.
3. Classify the AI system as high-risk if both conditions (a) and (b) are met.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 6, Paragraph 1: 'Irrespective of whether an AI system is placed on the market or put into service independently of the products referred to in points (a) and (b), that AI system shall be considered to be high-risk where both of the following conditions are fulfilled:

- (a)  
the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I;

(b)

the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-013: Identify High-Risk AI Systems Listed in Annex III

### Control Objective:

To ensure that AI systems listed in Annex III are classified as high-risk.

### Implementation Guidance:

1. Review the list of AI systems in Annex III.
2. Classify any AI system developed or used by the company that falls under the categories listed in Annex III as high-risk.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 6, Paragraph 2: 'In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall be considered to be high-risk.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-014: Assess Risk of Harm and Influence on Decision Making

### Control Objective:

To ensure that AI systems referred to in Annex III are properly assessed for their risk of harm and influence on decision making.

### Implementation Guidance:

1. Conduct a comprehensive risk assessment to determine if the AI system poses a significant risk of harm to the health, safety, or fundamental rights of natural persons.
2. Evaluate the AI system's potential to materially influence the outcome of decision making.
3. If the AI system does not pose a significant risk of harm and does not materially influence decision making, and it meets one of the conditions (a) through (d), it may be classified as not high-risk.
4. If the AI system performs profiling of natural persons, it shall always be considered high-risk, regardless of other factors.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 6, Paragraph 3: 'By derogation from paragraph 2, an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.'

The first subparagraph shall apply where any of the following conditions is fulfilled:

- (a)  
the AI system is intended to perform a narrow procedural task;
- (b)  
the AI system is intended to improve the result of a previously completed human activity;
- (c)

---

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or

(d)

the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

Notwithstanding the first subparagraph, an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-015: Document Risk Assessment for Non-High-Risk AI Systems

### Control Objective:

To ensure that providers document their assessment of AI systems classified as not high-risk.

### Implementation Guidance:

1. Develop a comprehensive documentation process for recording the risk assessment of AI systems classified as not high-risk.
2. Ensure that the documentation includes a clear justification for the classification as not high-risk, based on the criteria outlined in Article 6, Paragraph 3.
3. Maintain the documentation throughout the lifecycle of the AI system and make it available to national competent authorities upon request.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 6, Paragraph 4: 'A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Such provider shall be subject to the registration obligation set out in Article 49(2). Upon request of national competent authorities, the provider shall provide the documentation of the assessment.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 Requirements for high-risk AI systems, Article 8 Compliance with the requirements

### Compliance with Requirements for High-Risk AI Systems

*To ensure that high-risk AI systems comply with the requirements laid down in the regulation, taking into account their intended purpose and the state of the art in AI and related technologies.*

#### AIAct-016: Compliance with High-Risk AI System Requirements

##### Control Objective:

To ensure that high-risk AI systems comply with the requirements laid down in the regulation, taking into account their intended purpose and the state of the art in AI and related technologies.

##### Implementation Guidance:

1. Conduct a thorough risk assessment of the AI system, considering its intended purpose and the state of the art in AI and related technologies.
2. Implement a risk management system to address the identified risks.
3. Ensure that the AI system complies with all applicable requirements laid down in the regulation.
4. Regularly review and update the risk assessment and risk management system to reflect changes in the AI system, its intended purpose, and the state of the art in AI and related technologies.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 8, Section 1: 'High-risk AI systems shall comply with the requirements laid down in this Section, taking into account their intended purpose as well as the generally acknowledged state of the art on AI and AI-related technologies. The risk management system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.'

DRAFT



## AIAct-017: Compliance with Union Harmonisation Legislation

### Control Objective:

To ensure that products containing AI systems comply with all applicable requirements under Union harmonisation legislation.

### Implementation Guidance:

1. Identify all applicable Union harmonisation legislation for the product containing the AI system.
2. Ensure that the product is fully compliant with all applicable requirements under the identified legislation.
3. Integrate, as appropriate, the necessary testing and reporting processes, information, and documentation into existing documentation and procedures required under the Union harmonisation legislation.
4. Maintain records of compliance with Union harmonisation legislation.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 8, Section 2: 'Where a product contains an AI system, to which the requirements of this Regulation as well as requirements of the Union harmonisation legislation listed in Section A of Annex I apply, providers shall be responsible for ensuring that their product is fully compliant with all applicable requirements under applicable Union harmonisation legislation. In ensuring the compliance of high-risk AI systems referred to in paragraph 1 with the requirements set out in this Section, and in order to ensure consistency, avoid duplication and minimise additional burdens, providers shall have a choice of integrating, as appropriate, the necessary testing and reporting processes, information and documentation they provide with regard to their product into documentation and procedures that already exist and are required under the Union harmonisation legislation listed in Section A of Annex I.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 Requirements for high-risk AI systems, Article 9 Risk management system

### Risk Management System for High-Risk AI Systems

*To establish and maintain a comprehensive risk management system for high-risk AI systems, ensuring their safe and responsible development, deployment, and use.*

#### AIAct-018: Establish and Maintain Risk Management System for High-Risk AI Systems

##### Control Objective:

To ensure that a comprehensive risk management system is established, implemented, documented, and maintained for high-risk AI systems.

##### Implementation Guidance:

1. Develop a comprehensive risk management system specifically for high-risk AI systems.
2. Implement the risk management system throughout the entire lifecycle of the high-risk AI system.
3. Document the risk management system and its processes.
4. Regularly review and update the risk management system to ensure its effectiveness and relevance.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 9, Paragraph 1: A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-019: Implement Continuous Iterative Risk Management Process

### Control Objective:

To ensure that the risk management system is a continuous iterative process that is planned, run, and regularly reviewed and updated throughout the entire lifecycle of the high-risk AI system.

### Implementation Guidance:

1. Plan and execute the risk management process as a continuous iterative cycle.
2. Regularly review and update the risk management system based on new information, changes in the system, or evolving risks.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 2: The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-020: Identify and Analyze Known and Foreseeable Risks

### Control Objective:

To identify and analyze all known and reasonably foreseeable risks that the high-risk AI system can pose to health, safety, or fundamental rights when used as intended.

### Implementation Guidance:

1. Conduct a thorough risk identification process to identify all potential risks associated with the high-risk AI system.
2. Analyze the identified risks, considering their likelihood and potential impact on health, safety, and fundamental rights.
3. Document the risk identification and analysis process, including the identified risks and their associated likelihood and impact.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 2(a): the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-021: Estimate and Evaluate Risks under Intended Use and Misuse

### Control Objective:

To estimate and evaluate the risks that may arise when the high-risk AI system is used as intended and under conditions of reasonably foreseeable misuse.

### Implementation Guidance:

1. Estimate the likelihood and impact of risks associated with the intended use of the high-risk AI system.
2. Evaluate the risks that may emerge under conditions of reasonably foreseeable misuse, considering potential scenarios and user behavior.
3. Document the risk estimation and evaluation process, including the assessed risks and their associated likelihood and impact.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 2(b): the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-022: Evaluate Risks Based on Post-Market Monitoring Data

### Control Objective:

To evaluate potential risks based on the analysis of data gathered from the post-market monitoring system.

### Implementation Guidance:

1. Establish a post-market monitoring system to collect data on the use of the high-risk AI system.
2. Analyze the collected data to identify any emerging risks or potential issues.
3. Evaluate the identified risks based on their likelihood and impact, and take appropriate action to mitigate them.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 2(c): the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-023: Adopt Appropriate Risk Management Measures

### Control Objective:

To adopt appropriate and targeted risk management measures to address the identified risks.

### Implementation Guidance:

1. Develop and implement risk management measures that are specifically designed to address the identified risks.
2. Ensure that the risk management measures are appropriate for the nature and severity of the risks.
3. Document the adopted risk management measures, including their rationale and implementation details.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 2(d): the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-024: Focus on Mitigable or Eliminate Risks

### Control Objective:

To focus the risk management system on risks that can be reasonably mitigated or eliminated through design, development, or technical information.

### Implementation Guidance:

1. Prioritize risks that can be effectively addressed through design, development, or technical information.
2. Exclude risks that are not reasonably mitigable or eliminable through these means.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 3: The risks referred to in this Article shall concern only those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-025: Consider Combined Effects of Requirements

### Control Objective:

To consider the combined effects and interactions of the requirements set out in this Section when implementing risk management measures.

### Implementation Guidance:

1. Analyze the potential interactions and combined effects of the requirements in this Section.
2. Design risk management measures that effectively minimize risks while achieving a balance in fulfilling the requirements.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 4: The risk management measures referred to in paragraph 2, point (d), shall give due consideration to the effects and possible interaction resulting from the combined application of the requirements set out in this Section, with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-026: Ensure Acceptable Residual Risk

### Control Objective:

To ensure that the residual risk associated with each hazard and the overall residual risk of the high-risk AI system are judged to be acceptable.

### Implementation Guidance:

1. Evaluate the residual risk after implementing risk management measures.
2. Determine whether the residual risk is acceptable based on established risk tolerance levels.
3. Document the residual risk assessment and the rationale for its acceptability.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 5: The risk management measures referred to in paragraph 2, point (d), shall be such that the relevant residual risk associated with each hazard, as well as the overall residual risk of the high-risk AI systems is judged to be acceptable.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-027: Eliminate or Reduce Risks Through Design and Development

### Control Objective:

To eliminate or reduce identified risks as far as technically feasible through adequate design and development of the high-risk AI system.

### Implementation Guidance:

1. Incorporate risk mitigation strategies into the design and development process of the high-risk AI system.
2. Ensure that the design and development process is robust and effective in addressing identified risks.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 5(a): elimination or reduction of risks identified and evaluated pursuant to paragraph 2 in as far as technically feasible through adequate design and development of the high-risk AI system;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-028: Implement Mitigation and Control Measures for Unmitigable Risks

### Control Objective:

To implement adequate mitigation and control measures for risks that cannot be eliminated through design and development.

### Implementation Guidance:

1. Identify and implement appropriate mitigation and control measures for risks that cannot be eliminated.
2. Ensure that the mitigation and control measures are effective in reducing the likelihood and impact of the risks.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 5(b): where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-029: Provide Information and Training to Deployers

### Control Objective:

To provide deployers with the necessary information and training to understand and manage the risks associated with the high-risk AI system.

### Implementation Guidance:

1. Provide deployers with clear and comprehensive information about the high-risk AI system, including its intended purpose, potential risks, and mitigation measures.
2. Offer appropriate training to deployers on how to safely and responsibly use the high-risk AI system.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 5(c): provision of information required pursuant to Article 13 and, where appropriate, training to deployers.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-030: Test High-Risk AI Systems for Risk Management

### Control Objective:

To test high-risk AI systems to identify the most appropriate and targeted risk management measures and ensure consistent performance and compliance with requirements.

### Implementation Guidance:

1. Conduct thorough testing of the high-risk AI system to identify potential risks and vulnerabilities.
2. Ensure that the testing process is designed to assess the system's performance and compliance with the requirements set out in this Section.
3. Use the test results to inform the development of appropriate and targeted risk management measures.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 6: High-risk AI systems shall be tested for the purpose of identifying the most appropriate and targeted risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they are in compliance with the requirements set out in this Section.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-031: Consider Real-World Testing

### Control Objective:

To consider testing the high-risk AI system in real-world conditions, in accordance with Article 60, to gather reliable data and assess its performance.

### Implementation Guidance:

1. Evaluate the feasibility and appropriateness of conducting real-world testing of the high-risk AI system.
2. If real-world testing is deemed necessary, ensure that it is conducted in accordance with the requirements of Article 60.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 7: Testing procedures may include testing in real-world conditions in accordance with Article 60.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-032: Test Throughout Development and Before Market Release

### Control Objective:

To test high-risk AI systems throughout the development process and prior to market release, using defined metrics and probabilistic thresholds.

### Implementation Guidance:

1. Conduct testing at various stages of the development process, as appropriate.
2. Ensure that testing is completed prior to placing the high-risk AI system on the market or putting it into service.
3. Define clear metrics and probabilistic thresholds for testing, based on the intended purpose of the system.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 8: The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process, and, in any event, prior to their being placed on the market or put into service. Testing shall be carried out against prior defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-033: Consider Impact on Vulnerable Groups

### Control Objective:

To consider the potential adverse impact of the high-risk AI system on persons under the age of 18 and other vulnerable groups.

### Implementation Guidance:

1. Assess the potential risks and impacts of the high-risk AI system on persons under the age of 18 and other vulnerable groups.
2. Implement appropriate risk mitigation measures to address any potential adverse impacts on these groups.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 9: When implementing the risk management system as provided for in paragraphs 1 to 7, providers shall give consideration to whether in view of its intended purpose the high-risk AI system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-034: Integrate Risk Management with Other Legal Requirements

### Control Objective:

To integrate the risk management requirements of this Article with other relevant provisions of Union law regarding internal risk management processes.

### Implementation Guidance:

1. Review other relevant provisions of Union law that apply to internal risk management processes.
2. Integrate the requirements of this Article into existing risk management procedures, or develop new procedures that incorporate all relevant legal requirements.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 9, Paragraph 10: For providers of high-risk AI systems that are subject to requirements regarding internal risk management processes under other relevant provisions of Union law, the aspects provided in paragraphs 1 to 9 may be part of, or combined with, the risk management procedures established pursuant to that law.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 Requirements for high-risk AI systems, Article 10 Data and data governance

### Data and Data Governance for High-Risk AI Systems

*To ensure that high-risk AI systems are developed using training, validation, and testing data sets that meet specific quality criteria and are subject to appropriate data governance and management practices.*

#### AIAct-035: Ensure Data Set Quality for High-Risk AI System Development

##### Control Objective:

To ensure that high-risk AI systems are developed using training, validation, and testing data sets that meet specific quality criteria.

##### Implementation Guidance:

1. Establish a process to identify and document the specific quality criteria for training, validation, and testing data sets used in the development of high-risk AI systems.
2. Implement procedures to ensure that all data sets used in the development of high-risk AI systems meet the identified quality criteria.
3. Maintain records of data set quality assessments and any corrective actions taken to address identified deficiencies.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 10(1): High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-036: Implement Data Governance and Management Practices for High-Risk AI Systems

### Control Objective:

To ensure that training, validation, and testing data sets used in the development of high-risk AI systems are subject to appropriate data governance and management practices.

### Implementation Guidance:

1. Develop and implement a comprehensive data governance framework that addresses the specific requirements outlined in Article 10(2).
2. Establish clear policies and procedures for data collection, storage, processing, and use, ensuring alignment with the intended purpose of the high-risk AI system.
3. Implement appropriate data security measures to protect the confidentiality, integrity, and availability of training, validation, and testing data sets.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2): Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system. Those practices shall concern in particular:

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-037: Document and Review Design Choices for High-Risk AI Systems

### Control Objective:

To ensure that relevant design choices are documented and reviewed in relation to the development of high-risk AI systems.

### Implementation Guidance:

1. Establish a process for documenting all relevant design choices made during the development of high-risk AI systems.
2. Implement a review process to ensure that design choices are appropriate and aligned with the intended purpose of the high-risk AI system.
3. Maintain records of design choices and review findings.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2)(a): the relevant design choices;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-038: Document Data Collection Processes and Origin for High-Risk AI Systems

### Control Objective:

To ensure that data collection processes and the origin of data are documented, particularly for personal data, including the original purpose of collection.

### Implementation Guidance:

1. Establish a process for documenting data collection processes and the origin of data used in the development of high-risk AI systems.
2. For personal data, ensure that the original purpose of data collection is documented and that processing remains aligned with that purpose.
3. Maintain records of data collection processes, origin, and original purpose of collection for personal data.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2)(b): data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-039: Document Data Preparation Processing Operations for High-Risk AI Systems

### Control Objective:

To ensure that relevant data preparation processing operations are documented for high-risk AI systems.

### Implementation Guidance:

1. Establish a process for documenting all data preparation processing operations, including annotation, labelling, cleaning, updating, enrichment, and aggregation.
2. Ensure that documentation includes details about the methods and tools used for each operation.
3. Maintain records of data preparation processing operations and any changes made to the process.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2)(c): relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-040: Document and Review Assumptions about Data for High-Risk AI Systems

### Control Objective:

To ensure that assumptions about the information that data are supposed to measure and represent are documented and reviewed for high-risk AI systems.

### Implementation Guidance:

1. Establish a process for documenting all assumptions made about the information that data are supposed to measure and represent.
2. Implement a review process to ensure that assumptions are reasonable and supported by evidence.
3. Maintain records of assumptions and review findings.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2)(d): the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-041: Assess Data Set Availability, Quantity, and Suitability for High-Risk AI Systems

### Control Objective:

To ensure that the availability, quantity, and suitability of data sets are assessed for high-risk AI systems.

### Implementation Guidance:

1. Establish a process for assessing the availability, quantity, and suitability of data sets needed for the development of high-risk AI systems.
2. Ensure that assessments are conducted before and during the development process to identify any potential data gaps or shortcomings.
3. Maintain records of data set assessments and any corrective actions taken to address identified issues.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2)(e): an assessment of the availability, quantity and suitability of the data sets that are needed;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-042: Examine Data Sets for Potential Biases in High-Risk AI Systems

### Control Objective:

To ensure that data sets are examined for potential biases that could affect health and safety, fundamental rights, or lead to discrimination.

### Implementation Guidance:

1. Establish a process for examining data sets for potential biases that could affect health and safety, fundamental rights, or lead to discrimination.
2. Implement methods for identifying and assessing potential biases, including statistical analysis and expert review.
3. Maintain records of bias assessments and any corrective actions taken to mitigate identified biases.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2)(f): examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-043: Implement Measures to Detect, Prevent, and Mitigate Biases in High-Risk AI Systems

### Control Objective:

To ensure that appropriate measures are implemented to detect, prevent, and mitigate potential biases identified in data sets.

### Implementation Guidance:

1. Develop and implement a comprehensive bias mitigation strategy that includes measures for detection, prevention, and mitigation.
2. Ensure that bias mitigation measures are integrated into the development process and are continuously monitored and evaluated.
3. Maintain records of bias mitigation measures implemented and their effectiveness.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2)(g): appropriate measures to detect, prevent and mitigate possible biases identified according to point (f);

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-044: Identify and Address Data Gaps and Shortcomings for High-Risk AI Systems

### Control Objective:

To ensure that relevant data gaps or shortcomings that prevent compliance with the regulation are identified and addressed.

### Implementation Guidance:

1. Establish a process for identifying relevant data gaps or shortcomings that could prevent compliance with the regulation.
2. Develop and implement strategies to address identified gaps and shortcomings, including data collection, data augmentation, or alternative data sources.
3. Maintain records of data gap and shortcoming assessments and the actions taken to address them.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(2)(h): the identification of relevant data gaps or shortcomings that prevent compliance with this Regulation, and how those gaps and shortcomings can be addressed.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-045: Ensure Data Set Relevance, Representativeness, Accuracy, and Completeness for High-Risk AI Systems

### Control Objective:

To ensure that training, validation, and testing data sets are relevant, sufficiently representative, free of errors, and complete in view of the intended purpose.

### Implementation Guidance:

1. Establish a process for evaluating the relevance, representativeness, accuracy, and completeness of data sets used in the development of high-risk AI systems.
2. Implement methods for assessing statistical properties of data sets, including those related to the persons or groups of persons the AI system is intended to be used with.
3. Maintain records of data set evaluations and any corrective actions taken to address identified issues.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(3): Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-046: Consider Geographical, Contextual, Behavioral, and Functional Settings for High-Risk AI Systems

### Control Objective:

To ensure that data sets take into account the specific geographical, contextual, behavioral, and functional settings within which the high-risk AI system is intended to be used.

### Implementation Guidance:

1. Establish a process for identifying and documenting the specific geographical, contextual, behavioral, and functional settings within which the high-risk AI system is intended to be used.
2. Ensure that data sets are selected or created to reflect the characteristics and elements of those settings.
3. Maintain records of the identified settings and the rationale for data set selection or creation.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(4): Data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-047: Process Special Categories of Personal Data for Bias Detection and Correction in High-Risk AI Systems

### Control Objective:

To ensure that the processing of special categories of personal data for bias detection and correction in high-risk AI systems is strictly necessary and complies with all applicable legal requirements.

### Implementation Guidance:

1. Establish a process for determining whether the processing of special categories of personal data is strictly necessary for bias detection and correction.
2. Ensure that all conditions outlined in Article 10(5) are met before processing special categories of personal data.
3. Implement appropriate safeguards to protect the fundamental rights and freedoms of natural persons when processing special categories of personal data.
4. Maintain records of the rationale for processing special categories of personal data and the implemented safeguards.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(5): To the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems in accordance with paragraph (2), points (f) and (g) of this Article, the providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. In addition to the provisions set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, all the following conditions must be met in order for such processing to occur:

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## **AIAct-048: Demonstrate Necessity of Special Categories of Personal Data for Bias Detection and Correction**

### **Control Objective:**

To ensure that the processing of special categories of personal data for bias detection and correction is demonstrated to be strictly necessary and cannot be effectively fulfilled by processing other data.

### **Implementation Guidance:**

1. Establish a process for demonstrating that bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymized data.
2. Document the rationale for using special categories of personal data, including the specific limitations of alternative data sources.
3. Maintain records of the assessment and the rationale for using special categories of personal data.

### **Implementation Status:**

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### **AIAct requirement statement:**

Article 10(5)(a): the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-049: Implement Technical Limitations and Privacy-Preserving Measures for Special Categories of Personal Data

### Control Objective:

To ensure that special categories of personal data are subject to technical limitations on re-use and state-of-the-art security and privacy-preserving measures.

### Implementation Guidance:

1. Implement technical limitations on the re-use of special categories of personal data, restricting their use to the specific purpose of bias detection and correction.
2. Employ state-of-the-art security and privacy-preserving measures, including pseudonymisation, to protect the confidentiality and integrity of special categories of personal data.
3. Maintain records of implemented technical limitations and privacy-preserving measures.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(5)(b): the special categories of personal data are subject to technical limitations on the re-use of the personal data, and state-of-the-art security and privacy-preserving measures, including pseudonymisation;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-050: Secure and Protect Special Categories of Personal Data with Strict Controls and Access Documentation

### Control Objective:

To ensure that special categories of personal data are secured, protected, and subject to suitable safeguards, including strict controls and documentation of access.

### Implementation Guidance:

1. Implement robust security measures to protect special categories of personal data from unauthorized access, use, disclosure, alteration, or destruction.
2. Establish strict controls over access to special categories of personal data, ensuring that only authorized personnel have access with appropriate confidentiality obligations.
3. Maintain detailed documentation of all access to special categories of personal data, including the date, time, user, and purpose of access.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(5)(c): the special categories of personal data are subject to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-051: Restrict Transmission, Transfer, and Access of Special Categories of Personal Data

### Control Objective:

To ensure that special categories of personal data are not transmitted, transferred, or otherwise accessed by other parties.

### Implementation Guidance:

1. Establish clear policies and procedures prohibiting the transmission, transfer, or access of special categories of personal data to other parties.
2. Implement technical controls to prevent unauthorized sharing or access to special categories of personal data.
3. Maintain records of all data transfers and access requests for special categories of personal data.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(5)(d): the special categories of personal data are not to be transmitted, transferred or otherwise accessed by other parties;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-052: Delete Special Categories of Personal Data After Bias Correction or Retention Period

### Control Objective:

To ensure that special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period.

### Implementation Guidance:

1. Establish a process for deleting special categories of personal data once the bias has been corrected or the personal data has reached the end of its retention period.
2. Implement secure data deletion procedures to ensure that data is permanently removed from all systems and storage locations.
3. Maintain records of data deletion activities, including the date, time, and reason for deletion.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(5)(e): the special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-053: Document Rationale for Processing Special Categories of Personal Data for Bias Detection and Correction

### Control Objective:

To ensure that records of processing activities include the reasons why the processing of special categories of personal data was strictly necessary for bias detection and correction.

### Implementation Guidance:

1. Maintain detailed records of processing activities related to special categories of personal data, including the specific reasons why such processing was strictly necessary for bias detection and correction.
2. Document the rationale for why the objective of bias detection and correction could not be achieved by processing other data.
3. Ensure that records are readily available for review by relevant authorities.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(5)(f): the records of processing activities pursuant to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-054: Apply Data Governance and Management Practices to Testing Data Sets for High-Risk AI Systems Without Training

### Control Objective:

To ensure that data governance and management practices outlined in Article 10(2) to 10(5) are applied to testing data sets for high-risk AI systems that do not involve training of AI models.

### Implementation Guidance:

1. Establish a process for applying the data governance and management practices outlined in Article 10(2) to 10(5) specifically to testing data sets used in the development of high-risk AI systems that do not involve training of AI models.
2. Ensure that all requirements related to data quality, bias assessment, and data protection are met for testing data sets.
3. Maintain records of data governance and management activities related to testing data sets.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 10(6): For the development of high-risk AI systems not using techniques involving the training of AI models, paragraphs 2 to 5 apply only to the testing data sets.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 Requirements for high-risk AI systems, Article 11 Technical documentation

### Technical Documentation Requirements

*To ensure that high-risk AI systems are adequately documented to demonstrate compliance with regulatory requirements and facilitate assessment by authorities.*

#### AIAct-055: Develop and Maintain Technical Documentation for High-Risk AI Systems

##### Control Objective:

To ensure that comprehensive and up-to-date technical documentation is available for all high-risk AI systems.

##### Implementation Guidance:

1. Develop a detailed technical documentation package for each high-risk AI system before it is placed on the market or put into service.
2. Ensure that the documentation includes all the elements specified in Annex IV.
3. Maintain the technical documentation and update it regularly to reflect any changes to the AI system or its intended purpose.
4. Make the technical documentation readily available to national competent authorities and notified bodies upon request.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 11, Section 1: 'The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-056: Ensure Technical Documentation Demonstrates Compliance

### Control Objective:

To ensure that the technical documentation clearly and comprehensively demonstrates the AI system's compliance with regulatory requirements.

### Implementation Guidance:

1. Structure the technical documentation in a way that clearly and logically presents the information.
2. Use clear and concise language that is easily understandable by national competent authorities and notified bodies.
3. Provide sufficient evidence and supporting documentation to demonstrate compliance with all relevant requirements.
4. Ensure that the documentation is readily accessible and easily searchable.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 11, Section 1: 'The technical documentation shall be drawn up in such a way as to demonstrate that the high-risk AI system complies with the requirements set out in this Section and to provide national competent authorities and notified bodies with the necessary information in a clear and comprehensive form to assess the compliance of the AI system with those requirements.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-057: Include Required Elements in Technical Documentation

### Control Objective:

To ensure that the technical documentation includes all the mandatory elements specified in Annex IV.

### Implementation Guidance:

1. Review Annex IV to identify all the required elements for technical documentation.
2. Ensure that each element is included in the technical documentation for all high-risk AI systems.
3. Provide detailed and accurate information for each element, as specified in Annex IV.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 11, Section 1: 'It shall contain, at a minimum, the elements set out in Annex IV.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-058: Simplified Technical Documentation for SMEs

### Control Objective:

To allow SMEs to provide simplified technical documentation for high-risk AI systems.

### Implementation Guidance:

1. If the company is an SME, including a start-up, it may provide the technical documentation in a simplified manner.
2. Utilize the simplified technical documentation form established by the Commission for SMEs.
3. Ensure that the simplified documentation still provides all the essential information required for compliance assessment.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 11, Section 1: 'SMEs, including start-ups, may provide the elements of the technical documentation specified in Annex IV in a simplified manner.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-059: Consolidated Technical Documentation for Combined Products

### Control Objective:

To ensure that a single set of technical documentation is provided for high-risk AI systems related to products covered by Union harmonisation legislation.

### Implementation Guidance:

1. If the high-risk AI system is related to a product covered by Union harmonisation legislation listed in Section A of Annex I, combine all the required information into a single set of technical documentation.
2. Include all the information specified in paragraph 1 of Article 11, as well as the information required under the relevant Union harmonisation legislation.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 11, Section 2: 'Where a high-risk AI system related to a product covered by the Union harmonisation legislation listed in Section A of Annex I is placed on the market or put into service, a single set of technical documentation shall be drawn up containing all the information set out in paragraph 1, as well as the information required under those legal acts.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 Requirements for high-risk AI systems, Article 12 Record-keeping

### Record-keeping for High-Risk AI Systems

*To ensure traceability of the functioning of high-risk AI systems, enabling identification of potential risks, post-market monitoring, and operational monitoring.*

#### AIAct-060: Implement Logging Capabilities for High-Risk AI Systems

##### Control Objective:

To ensure that high-risk AI systems are equipped with logging capabilities to record events throughout their lifetime.

##### Implementation Guidance:

1. Design and implement technical features within high-risk AI systems to enable automatic recording of events (logs).
2. Ensure that the logging capabilities are operational throughout the entire lifespan of the AI system.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 12(1): High-risk AI systems shall technically allow for the automatic recording of events (logs) over the lifetime of the system.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-061: Log Events Relevant for Traceability and Monitoring

### Control Objective:

To ensure that logging capabilities capture events relevant for traceability, risk identification, post-market monitoring, and operational monitoring.

### Implementation Guidance:

1. Define and document the specific events that need to be logged to ensure traceability and facilitate monitoring.
2. Configure logging capabilities to capture events related to:

- \* Identifying situations that may lead to risks or substantial modifications.
- \* Facilitating post-market monitoring.
- \* Monitoring the operation of high-risk AI systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 12(2): In order to ensure a level of traceability of the functioning of a high-risk AI system that is appropriate to the intended purpose of the system, logging capabilities shall enable the recording of events relevant for:

- (a) identifying situations that may result in the high-risk AI system presenting a risk within the meaning of Article 79(1) or in a substantial modification;
- (b) facilitating the post-market monitoring referred to in Article 72; and
- (c) monitoring the operation of high-risk AI systems referred to in Article 26(5).

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-062: Implement Minimum Logging Requirements for Specific High-Risk AI Systems

### Control Objective:

To ensure that logging capabilities for specific high-risk AI systems capture essential information for traceability and accountability.

### Implementation Guidance:

1. For high-risk AI systems listed in Annex III, point 1(a), implement logging capabilities that capture the following information at a minimum:

- \* Start and end dates and times of each system use.
- \* Reference database used for input data checking.
- \* Input data that resulted in a match.
- \* Identification of natural persons involved in result verification (as per Article 14(5)).

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 12(3): For high-risk AI systems referred to in point 1 (a), of Annex III, the logging capabilities shall provide, at a minimum:

(a) recording of the period of each use of the system (start date and time and end date and time of each use);

(b) the reference database against which input data has been checked by the system;

(c) the input data for which the search has led to a match;

(d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14(5).

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

DRAFT

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 Requirements for high-risk AI systems, Article 13 Transparency and provision of information to deployers

### Transparency and Provision of Information to Deployers

*To ensure that high-risk AI systems are designed and developed with sufficient transparency to enable deployers to understand the system's output and use it appropriately.*

#### AIAct-063: Ensure Transparency in High-Risk AI System Design and Development

##### Control Objective:

To ensure that high-risk AI systems are designed and developed with sufficient transparency to enable deployers to understand the system's output and use it appropriately.

##### Implementation Guidance:

1. Design and develop high-risk AI systems with transparency in mind, ensuring that their operation is sufficiently transparent to enable deployers to interpret the system's output and use it appropriately.
2. Implement measures to achieve an appropriate type and degree of transparency, taking into account the relevant obligations of the provider and deployer set out in Section 3.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 13, Section 1: 'High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured with a view to achieving compliance with the relevant obligations of the provider and deployer set out in Section 3.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-064: Provide Instructions for Use for High-Risk AI Systems

### Control Objective:

To ensure that high-risk AI systems are accompanied by clear and comprehensive instructions for use.

### Implementation Guidance:

1. Provide instructions for use for high-risk AI systems in an appropriate digital format or otherwise.
2. Ensure that the instructions for use are concise, complete, correct, clear, relevant, accessible, and comprehensible to deployers.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 13, Section 2: 'High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-065: Provide Provider Identity and Contact Information

### Control Objective:

To ensure that the instructions for use include the identity and contact details of the provider and, where applicable, its authorized representative.

### Implementation Guidance:

1. Include the identity and contact details of the provider in the instructions for use.
2. If applicable, include the contact details of the provider's authorized representative in the instructions for use.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 13, Section 3(a): 'the identity and the contact details of the provider and, where applicable, of its authorised representative;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-066: Document High-Risk AI System Characteristics, Capabilities, and Limitations

### Control Objective:

To ensure that the instructions for use include detailed information about the characteristics, capabilities, and limitations of the high-risk AI system.

### Implementation Guidance:

1. Include a detailed description of the intended purpose of the high-risk AI system.
2. Provide information on the level of accuracy, including metrics, robustness, and cybersecurity, against which the system has been tested and validated.
3. Identify any known or foreseeable circumstances that may impact the expected level of accuracy, robustness, and cybersecurity.
4. Describe any known or foreseeable circumstances that may lead to risks to health, safety, or fundamental rights when using the system as intended or under conditions of reasonably foreseeable misuse.
5. If applicable, document the technical capabilities and characteristics of the system to provide information relevant to explaining its output.
6. When appropriate, provide information on the system's performance regarding specific persons or groups of persons.
7. When appropriate, include specifications for the input data and relevant information about the training, validation, and testing data sets used.
8. If applicable, provide information to enable deployers to interpret the system's output and use it appropriately.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 13, Section 3(b): 'the characteristics, capabilities and limitations of performance of the high-risk AI system, including:',

(i) 'its intended purpose;'

(ii) 'the level of accuracy, including its metrics, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that

---

[LinkedIn post has number of pages restriction. Full version download information can be found on the last page.](#)

expected level of accuracy, robustness and cybersecurity;'

(iii) 'any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights referred to in Article 9(2);'

(iv) 'where applicable, the technical capabilities and characteristics of the high-risk AI system to provide information that is relevant to explain its output;'

(v) 'when appropriate, its performance regarding specific persons or groups of persons on which the system is intended to be used;'

(vi) 'when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the high-risk AI system;'

(vii) 'where applicable, information to enable deployers to interpret the output of the high-risk AI system and use it appropriately;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-067: Document Pre-Determined Changes to High-Risk AI System

### Control Objective:

To ensure that the instructions for use include information about any pre-determined changes to the high-risk AI system and its performance.

### Implementation Guidance:

1. Document any changes to the high-risk AI system and its performance that were pre-determined by the provider at the time of the initial conformity assessment.
2. Include this information in the instructions for use.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 13, Section 3(c): 'the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-068: Document Human Oversight Measures and Technical Support for Interpretation

### Control Objective:

To ensure that the instructions for use include information about human oversight measures and technical support for interpreting the outputs of the high-risk AI system.

### Implementation Guidance:

1. Document the human oversight measures implemented for the high-risk AI system, as outlined in Article 14.
2. Include information about the technical measures put in place to facilitate the interpretation of the system's outputs by deployers.
3. Include this information in the instructions for use.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 13, Section 3(d): 'the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of the high-risk AI systems by the deployers;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-069: Document Computational and Hardware Resources, Lifetime, and Maintenance Requirements

### Control Objective:

To ensure that the instructions for use include information about the computational and hardware resources needed, the expected lifetime of the high-risk AI system, and any necessary maintenance and care measures.

### Implementation Guidance:

1. Document the computational and hardware resources needed for the high-risk AI system.
2. Specify the expected lifetime of the system.
3. Outline any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of the system.
4. Include information about software updates.
5. Include this information in the instructions for use.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 13, Section 3(e): 'the computational and hardware resources needed, the expected lifetime of the high-risk AI system and any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of that AI system, including as regards software updates;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-070: Document Log Collection, Storage, and Interpretation Mechanisms

### Control Objective:

To ensure that the instructions for use include information about the mechanisms within the high-risk AI system that allow deployers to collect, store, and interpret logs.

### Implementation Guidance:

1. If relevant, provide a description of the mechanisms within the high-risk AI system that allow deployers to collect, store, and interpret logs.
2. Ensure that these mechanisms comply with the requirements outlined in Article 12.
3. Include this information in the instructions for use.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 13, Section 3(f): 'where relevant, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret the logs in accordance with Article 12.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 Requirements for high-risk AI systems, Article 14 Human oversight

### Human Oversight for High-Risk AI Systems

*To ensure that high-risk AI systems are designed and developed with appropriate human oversight mechanisms to mitigate risks to health, safety, and fundamental rights.*

#### AIAct-071: Design for Human Oversight

##### Control Objective:

To ensure that high-risk AI systems are designed and developed with appropriate human oversight mechanisms.

##### Implementation Guidance:

1. Implement design principles that prioritize human oversight throughout the AI system's lifecycle.
2. Develop human-machine interface tools that facilitate effective monitoring and intervention by human operators.
3. Ensure that the AI system's design allows for clear and understandable communication of its capabilities, limitations, and potential risks to human operators.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 14, Section 1: 'High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-072: Risk Mitigation through Human Oversight

### Control Objective:

To prevent or minimize risks to health, safety, and fundamental rights associated with high-risk AI systems.

### Implementation Guidance:

1. Conduct thorough risk assessments to identify potential risks to health, safety, and fundamental rights associated with the AI system.
2. Develop and implement human oversight mechanisms that effectively address identified risks.
3. Ensure that human oversight measures are proportionate to the level of risk and the AI system's autonomy.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 14, Section 2: 'Human oversight shall aim to prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular where such risks persist despite the application of other requirements set out in this Section.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-073: Implementation of Oversight Measures

### Control Objective:

To ensure that appropriate oversight measures are implemented for high-risk AI systems.

### Implementation Guidance:

1. Develop and implement oversight measures that are proportionate to the risks, level of autonomy, and context of use of the AI system.
2. Integrate oversight measures into the AI system's design, where technically feasible, before it is placed on the market or put into service.
3. Provide clear guidance and instructions to deployers on how to implement appropriate oversight measures.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 14, Section 3: 'The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the high-risk AI system, and shall be ensured through either one or both of the following types of measures:

(a)

measures identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;

(b)

measures identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the deployer.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-074: Enable Effective Human Oversight

### Control Objective:

To ensure that human operators are equipped to effectively oversee high-risk AI systems.

### Implementation Guidance:

1. Provide human operators with comprehensive training on the AI system's capabilities, limitations, and potential risks.
2. Equip human operators with appropriate tools and resources to monitor the AI system's operation and detect anomalies, dysfunctions, and unexpected performance.
3. Implement mechanisms to mitigate automation bias and ensure that human operators are not overly reliant on the AI system's output.
4. Provide human operators with clear guidance on how to interpret the AI system's output and make informed decisions.
5. Ensure that human operators have the authority to override or reverse the AI system's output in specific situations.
6. Implement emergency stop mechanisms that allow human operators to safely halt the AI system's operation.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 14, Section 4: 'For the purpose of implementing paragraphs 1, 2 and 3, the high-risk AI system shall be provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate:

(a)

to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance;

(b)

---

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

(c)

to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available;

(d)

to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system;

(e)

to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-075: Double Verification for High-Risk AI Systems

### Control Objective:

To ensure that decisions based on high-risk AI systems are subject to double verification by qualified individuals.

### Implementation Guidance:

1. Implement a double verification process for high-risk AI systems used for identification purposes, requiring confirmation by at least two qualified individuals.
2. Ensure that individuals involved in the verification process have the necessary competence, training, and authority to perform the task.
3. Document the verification process and maintain records of all verifications performed.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 14, Section 5: 'For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 of this Article shall be such as to ensure that, in addition, no action or decision is taken by the deployer on the basis of the identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority.'

The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 2 Requirements for high-risk AI systems, Article 15 Accuracy, robustness and cybersecurity

### Accuracy, Robustness, and Cybersecurity of High-Risk AI Systems

*To ensure that high-risk AI systems are designed and developed with appropriate levels of accuracy, robustness, and cybersecurity, and that they maintain these qualities throughout their lifecycle.*

#### AIAct-076: Ensure Accuracy, Robustness, and Cybersecurity of High-Risk AI Systems

##### Control Objective:

To ensure that high-risk AI systems meet the required levels of accuracy, robustness, and cybersecurity throughout their lifecycle.

##### Implementation Guidance:

1. Design and develop high-risk AI systems to achieve appropriate levels of accuracy, robustness, and cybersecurity.
2. Implement measures to ensure consistent performance in terms of accuracy, robustness, and cybersecurity throughout the system's lifecycle.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 15, Paragraph 1: High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-077: Declare Accuracy Metrics in Instructions for Use

### Control Objective:

To ensure that the levels of accuracy and relevant accuracy metrics of high-risk AI systems are clearly documented and provided to users.

### Implementation Guidance:

1. Include a clear declaration of the levels of accuracy and relevant accuracy metrics in the instructions for use accompanying high-risk AI systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 15, Paragraph 3: The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-078: Implement Resilience Measures for High-Risk AI Systems

### Control Objective:

To ensure that high-risk AI systems are resilient to errors, faults, and inconsistencies, particularly those arising from interactions with humans or other systems.

### Implementation Guidance:

1. Implement technical and organizational measures to enhance the resilience of high-risk AI systems against errors, faults, and inconsistencies.
2. Consider potential sources of errors, faults, or inconsistencies, including interactions with natural persons and other systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 15, Paragraph 4: High-risk AI systems shall be as resilient as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. Technical and organisational measures shall be taken in this regard.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-079: Implement Technical Redundancy Solutions

### Control Objective:

To enhance the robustness of high-risk AI systems by implementing technical redundancy solutions, such as backup or fail-safe plans.

### Implementation Guidance:

1. Explore and implement technical redundancy solutions, including backup or fail-safe plans, to improve the robustness of high-risk AI systems.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 15, Paragraph 4: The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-080: Mitigate Bias in Feedback Loops for Continuously Learning AI Systems

### Control Objective:

To minimize the risk of biased outputs influencing future operations (feedback loops) in high-risk AI systems that continue to learn after deployment.

### Implementation Guidance:

1. Develop high-risk AI systems that continue to learn after deployment in a way that minimizes the risk of biased outputs influencing future operations.
2. Implement appropriate mitigation measures to address any feedback loops that may arise.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 15, Paragraph 4: High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-081: Enhance Cybersecurity of High-Risk AI Systems

### Control Objective:

To ensure that high-risk AI systems are resilient against unauthorized attempts to alter their use, outputs, or performance by exploiting vulnerabilities.

### Implementation Guidance:

1. Implement measures to enhance the cybersecurity of high-risk AI systems, making them resilient against unauthorized attempts to alter their use, outputs, or performance.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 15, Paragraph 5: High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-082: Tailor Cybersecurity Solutions to Specific Risks

### Control Objective:

To ensure that cybersecurity solutions for high-risk AI systems are tailored to the specific circumstances and risks involved.

### Implementation Guidance:

1. Implement cybersecurity solutions for high-risk AI systems that are appropriate to the specific circumstances and risks involved.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 15, Paragraph 5: The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-083: Implement Measures to Address AI-Specific Vulnerabilities

### Control Objective:

To address AI-specific vulnerabilities by implementing measures to prevent, detect, respond to, resolve, and control attacks targeting training data, pre-trained components, inputs, confidentiality, or model flaws.

### Implementation Guidance:

1. Implement measures to prevent, detect, respond to, resolve, and control attacks targeting training data (data poisoning), pre-trained components (model poisoning), inputs (adversarial examples or model evasion), confidentiality, or model flaws.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 15, Paragraph 5: The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 Obligations of providers and deployers of high-risk AI systems and other parties, Article 16 Obligations of providers of high-risk AI systems

### Obligations of Providers of High-Risk AI Systems

*To outline the specific obligations that providers of high-risk AI systems must adhere to, ensuring compliance with the regulation and responsible development and deployment of these systems.*

#### AIAct-084: Ensure Compliance with High-Risk AI System Requirements

##### Control Objective:

To ensure that all high-risk AI systems developed and deployed by the company meet the requirements outlined in Section 2 of the regulation.

##### Implementation Guidance:

1. Conduct thorough assessments to verify that the high-risk AI system meets all the requirements specified in Section 2 of the regulation.
2. Implement a robust quality management system to ensure ongoing compliance with the requirements.
3. Establish a process for regular review and updates to the AI system to maintain compliance with evolving regulations and best practices.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 16 (a): Providers of high-risk AI systems shall ensure that their high-risk AI systems are compliant with the requirements set out in Section 2.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-085: Provide Clear Identification and Contact Information

### Control Objective:

To ensure that all high-risk AI systems are clearly identified with the provider's information, enabling traceability and accountability.

### Implementation Guidance:

1. Include the provider's name, registered trade name, or registered trademark on the AI system itself, its packaging, or accompanying documentation.
2. Provide a clear and accessible contact address for the provider, allowing for communication and inquiries related to the AI system.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (b): Providers of high-risk AI systems shall indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trade mark, the address at which they can be contacted.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-086: Implement a Compliant Quality Management System

### Control Objective:

To ensure that the company has a robust quality management system in place that meets the requirements of Article 17, promoting continuous improvement and compliance.

### Implementation Guidance:

1. Develop and implement a comprehensive quality management system that aligns with the requirements of Article 17.
2. Establish clear procedures for documenting, reviewing, and improving the quality management system.
3. Regularly audit the quality management system to ensure its effectiveness and compliance with Article 17.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (c): Providers of high-risk AI systems shall have a quality management system in place which complies with Article 17.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-087: Maintain Required Documentation for High-Risk AI Systems

### Control Objective:

To ensure that the company maintains all the documentation specified in Article 18, providing a comprehensive record of the AI system's development, testing, and deployment.

### Implementation Guidance:

1. Establish a system for collecting, organizing, and storing all documentation related to the high-risk AI system, as outlined in Article 18.
2. Ensure that the documentation is readily accessible and maintained throughout the AI system's lifecycle.
3. Implement procedures for updating and revising the documentation as necessary.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (d): Providers of high-risk AI systems shall keep the documentation referred to in Article 18.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-088: Maintain Logs of High-Risk AI System Activity

### Control Objective:

To ensure that the company maintains logs of all activity generated by the high-risk AI system, providing valuable insights for monitoring, troubleshooting, and auditing.

### Implementation Guidance:

1. Implement a system for capturing and storing logs generated by the high-risk AI system, as specified in Article 19.
2. Ensure that the logs are securely stored and protected from unauthorized access or modification.
3. Establish procedures for managing and analyzing the logs to identify potential issues or anomalies.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (e): Providers of high-risk AI systems shall, when under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-089: Conduct Conformity Assessment for High-Risk AI Systems

### Control Objective:

To ensure that the company conducts the necessary conformity assessment procedures outlined in Article 43 before placing the high-risk AI system on the market or putting it into service.

### Implementation Guidance:

1. Engage with a notified body or conduct internal conformity assessment, as required by Article 43, to verify the AI system's compliance with the regulation.
2. Ensure that the conformity assessment process is thorough and covers all relevant aspects of the AI system's design, development, and intended use.
3. Document the conformity assessment process and its findings, providing evidence of compliance.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (f): Providers of high-risk AI systems shall ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43, prior to its being placed on the market or put into service.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-090: Prepare EU Declaration of Conformity for High-Risk AI Systems

### Control Objective:

To ensure that the company prepares a comprehensive EU declaration of conformity, as outlined in Article 47, affirming the AI system's compliance with the regulation.

### Implementation Guidance:

1. Develop a detailed EU declaration of conformity that accurately reflects the AI system's characteristics and its compliance with the requirements of the regulation.
2. Ensure that the declaration of conformity is signed and dated by an authorized representative of the company.
3. Maintain a copy of the EU declaration of conformity and make it available to relevant authorities upon request.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (g): Providers of high-risk AI systems shall draw up an EU declaration of conformity in accordance with Article 47.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-091: Affix CE Marking to High-Risk AI Systems

### Control Objective:

To ensure that the company affixes the CE marking to the high-risk AI system, its packaging, or accompanying documentation, as required by Article 48, indicating compliance with the regulation.

### Implementation Guidance:

1. Apply the CE marking to the high-risk AI system itself, its packaging, or accompanying documentation, as specified in Article 48.
2. Ensure that the CE marking is clearly visible and legible, allowing for easy identification of the AI system's compliance status.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (h): Providers of high-risk AI systems shall affix the CE marking to the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, to indicate conformity with this Regulation, in accordance with Article 48.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-092: Comply with Registration Obligations for High-Risk AI Systems

### Control Objective:

To ensure that the company complies with the registration requirements outlined in Article 49(1), providing transparency and facilitating oversight of high-risk AI systems.

### Implementation Guidance:

1. Register the high-risk AI system with the designated authority, as specified in Article 49(1), providing all required information.
2. Maintain accurate and up-to-date registration information, ensuring timely updates as necessary.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (i): Providers of high-risk AI systems shall comply with the registration obligations referred to in Article 49(1).

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-093: Implement Corrective Actions and Provide Information for High-Risk AI Systems

### Control Objective:

To ensure that the company takes prompt and appropriate corrective actions and provides necessary information, as outlined in Article 20, in response to identified risks or issues related to the high-risk AI system.

### Implementation Guidance:

1. Establish a system for monitoring the high-risk AI system for potential risks or issues.
2. Implement corrective actions promptly and effectively to address any identified risks or issues, as required by Article 20.
3. Provide clear and timely information to relevant authorities and affected parties regarding any corrective actions taken.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (j): Providers of high-risk AI systems shall take the necessary corrective actions and provide information as required in Article 20.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-094: Demonstrate Conformity of High-Risk AI Systems to Competent Authorities

### Control Objective:

To ensure that the company is prepared to demonstrate the conformity of the high-risk AI system with the requirements of Section 2, upon a reasoned request from a national competent authority.

### Implementation Guidance:

1. Maintain comprehensive documentation and evidence to support the AI system's compliance with the requirements of Section 2.
2. Establish a process for responding to reasoned requests from national competent authorities, providing the necessary information and documentation to demonstrate conformity.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (k): Providers of high-risk AI systems shall, upon a reasoned request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Section 2.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-095: Ensure Accessibility of High-Risk AI Systems

### Control Objective:

To ensure that the company designs and develops the high-risk AI system in accordance with accessibility requirements outlined in Directives (EU) 2016/2102 and (EU) 2019/882, promoting inclusivity and usability for all.

### Implementation Guidance:

1. Conduct accessibility assessments throughout the AI system's development lifecycle, ensuring compliance with the requirements of Directives (EU) 2016/2102 and (EU) 2019/882.
2. Implement design principles and features that promote accessibility for users with disabilities.
3. Provide clear and accessible documentation and instructions for using the AI system.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 16 (l): Providers of high-risk AI systems shall ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 Obligations of providers and deployers of high-risk AI systems and other parties, Article 17 Quality management system

### Quality Management System for High-Risk AI Systems

*To establish a comprehensive quality management system for providers of high-risk AI systems, ensuring compliance with the regulation and promoting responsible development and deployment.*

#### AIAct-096: Establish a Quality Management System for High-Risk AI Systems

##### Control Objective:

To ensure compliance with the regulation through a documented and comprehensive quality management system.

##### Implementation Guidance:

1. Develop a documented quality management system that includes written policies, procedures, and instructions.
2. Ensure the system is systematic, orderly, and covers all aspects outlined in Article 17, Section 1.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 17, Section 1: 'Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-097: Develop a Regulatory Compliance Strategy

### Control Objective:

To ensure compliance with conformity assessment procedures and manage modifications to the high-risk AI system.

### Implementation Guidance:

1. Define a clear strategy for regulatory compliance, encompassing conformity assessment procedures.
2. Establish procedures for managing modifications to the high-risk AI system, ensuring ongoing compliance.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(a): 'a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-098: Implement Design Control and Verification Procedures

### Control Objective:

To ensure the design, control, and verification of the high-risk AI system meet regulatory requirements.

### Implementation Guidance:

1. Define techniques, procedures, and systematic actions for the design, control, and verification of the high-risk AI system.
2. Implement these procedures throughout the design process to ensure compliance.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(b): 'techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-099: Establish Development, Quality Control, and Assurance Procedures

### Control Objective:

To ensure the development, quality control, and quality assurance of the high-risk AI system meet regulatory standards.

### Implementation Guidance:

1. Define techniques, procedures, and systematic actions for the development, quality control, and quality assurance of the high-risk AI system.
2. Implement these procedures throughout the development process to ensure compliance.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(c): 'techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-100: Implement Examination, Testing, and Validation Procedures

### Control Objective:

To ensure the high-risk AI system undergoes thorough examination, testing, and validation throughout its development.

### Implementation Guidance:

1. Define procedures for examination, testing, and validation of the high-risk AI system before, during, and after development.
2. Establish the frequency of these procedures to ensure ongoing compliance.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(d): 'examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-101: Apply Technical Specifications and Standards

### Control Objective:

To ensure the high-risk AI system meets technical specifications and relevant standards.

### Implementation Guidance:

1. Identify and apply relevant technical specifications and standards, including harmonised standards.
2. If harmonised standards are not fully applicable, define alternative means to ensure compliance with the requirements.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(e): 'technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full or do not cover all of the relevant requirements set out in Section 2, the means to be used to ensure that the high-risk AI system complies with those requirements;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-102: Implement Data Management Systems and Procedures

### Control Objective:

To ensure responsible and compliant data management practices for high-risk AI systems.

### Implementation Guidance:

1. Establish systems and procedures for data management, covering all stages from acquisition to retention.
2. Ensure these systems and procedures comply with relevant data protection regulations and ethical guidelines.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(f): 'systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-103: Integrate Risk Management System

### Control Objective:

To ensure the quality management system incorporates a robust risk management system as outlined in Article 9.

### Implementation Guidance:

1. Integrate the risk management system described in Article 9 into the overall quality management system.
2. Ensure the risk management system is effectively implemented and maintained.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(g): 'the risk management system referred to in Article 9;' [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-104: Establish and Maintain a Post-Market Monitoring System

### Control Objective:

To ensure ongoing monitoring of high-risk AI systems after they are placed on the market or put into service.

### Implementation Guidance:

1. Establish a post-market monitoring system in accordance with Article 72.
2. Implement and maintain the system to collect and review experience gained from the use of the AI systems.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(h): 'the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 72;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-105: Implement Serious Incident Reporting Procedures

### Control Objective:

To ensure timely and accurate reporting of serious incidents related to high-risk AI systems.

### Implementation Guidance:

1. Develop procedures for reporting serious incidents in accordance with Article 73.
2. Ensure these procedures are communicated to relevant stakeholders and effectively implemented.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(i): 'procedures related to the reporting of a serious incident in accordance with Article 73;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-106: Establish Communication Procedures

### Control Objective:

To ensure effective communication with relevant authorities, stakeholders, and interested parties.

### Implementation Guidance:

1. Define procedures for handling communication with national competent authorities, other relevant authorities, notified bodies, operators, customers, and other interested parties.
2. Ensure these procedures are clear, efficient, and facilitate transparent communication.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(j): 'the handling of communication with national competent authorities, other relevant authorities, including those providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-107: Implement Record-Keeping Systems and Procedures

### Control Objective:

To ensure the systematic and secure record-keeping of all relevant documentation and information.

### Implementation Guidance:

1. Establish systems and procedures for record-keeping of all relevant documentation and information related to the high-risk AI system.
2. Ensure these systems and procedures are compliant with data protection regulations and maintain the integrity and confidentiality of the records.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(k): 'systems and procedures for record-keeping of all relevant documentation and information;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-108: Implement Resource Management and Security-of-Supply Measures

### Control Objective:

To ensure effective resource management and security of supply for the high-risk AI system.

### Implementation Guidance:

1. Establish procedures for resource management, including human resources, technical resources, and financial resources.
2. Implement security-of-supply related measures to ensure the continuous availability and reliability of the AI system.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(l): 'resource management, including security-of-supply related measures;'  
[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-109: Establish an Accountability Framework

### Control Objective:

To define clear responsibilities for management and staff regarding the quality management system.

### Implementation Guidance:

1. Develop an accountability framework that outlines the responsibilities of management and other staff for all aspects of the quality management system.
2. Ensure this framework is communicated to all relevant personnel and effectively implemented.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 1(m): 'an accountability framework setting out the responsibilities of the management and other staff with regard to all the aspects listed in this paragraph.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-110: Proportionate Implementation of Quality Management System

### Control Objective:

To ensure the implementation of the quality management system is proportionate to the size of the provider's organization.

### Implementation Guidance:

1. Conduct a risk assessment to determine the appropriate level of rigor and protection required for the quality management system based on the size and complexity of the provider's organization.
2. Implement the quality management system in a manner that is proportionate to the assessed risks and the provider's resources.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 2: 'The implementation of the aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation. Providers shall, in any event, respect the degree of rigour and the level of protection required to ensure the compliance of their high-risk AI systems with this Regulation.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-111: Integrate Quality Management System with Sectoral Union Law

### Control Objective:

To ensure compliance with relevant sectoral Union law regarding quality management systems.

### Implementation Guidance:

1. If subject to obligations regarding quality management systems under relevant sectoral Union law, integrate the aspects listed in Article 17, Section 1 into the existing quality management system.
2. Ensure the integrated system meets the requirements of both the regulation and the relevant sectoral Union law.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 3: 'Providers of high-risk AI systems that are subject to obligations regarding quality management systems or an equivalent function under relevant sectoral Union law may include the aspects listed in paragraph 1 as part of the quality management systems pursuant to that law.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-112: Fulfill Quality Management System Obligations for Financial Institutions

### Control Objective:

To ensure compliance with quality management system obligations for financial institutions subject to Union financial services law.

### Implementation Guidance:

1. If a financial institution, comply with the rules on internal governance arrangements or processes pursuant to relevant Union financial services law.
2. Ensure compliance with harmonised standards referred to in Article 40, particularly regarding the aspects of the quality management system not covered by internal governance arrangements or processes.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 17, Section 4: 'For providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the obligation to put in place a quality management system, with the exception of paragraph 1, points (g), (h) and (i) of this Article, shall be deemed to be fulfilled by complying with the rules on internal governance arrangements or processes pursuant to the relevant Union financial services law. To that end, any harmonised standards referred to in Article 40 shall be taken into account.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 Obligations of providers and deployers of high-risk AI systems and other parties, Article 18 Documentation keeping

### Documentation Keeping

*To ensure that providers of high-risk AI systems maintain adequate documentation for a specified period, facilitating oversight and accountability.*

#### AIAct-113: Maintain Documentation for High-Risk AI Systems

##### Control Objective:

To ensure that providers of high-risk AI systems maintain adequate documentation for a specified period, facilitating oversight and accountability.

##### Implementation Guidance:

1. Maintain technical documentation as specified in Article 11 for a period of 10 years after the high-risk AI system has been placed on the market or put into service.
2. Maintain documentation concerning the quality management system as specified in Article 17 for a period of 10 years after the high-risk AI system has been placed on the market or put into service.
3. Maintain documentation concerning changes approved by notified bodies, where applicable, for a period of 10 years after the high-risk AI system has been placed on the market or put into service.
4. Maintain decisions and other documents issued by notified bodies, where applicable, for a period of 10 years after the high-risk AI system has been placed on the market or put into service.
5. Maintain the EU declaration of conformity as specified in Article 47 for a period of 10 years after the high-risk AI system has been placed on the market or put into service.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

Article 18, Section 1: The provider shall, for a period ending 10 years after the high-risk AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities:

- (a) the technical documentation referred to in Article 11;
- (b) the documentation concerning the quality management system referred to in Article 17;
- (c) the documentation concerning the changes approved by notified bodies, where applicable;
- (d) the decisions and other documents issued by the notified bodies, where applicable;
- (e) the EU declaration of conformity referred to in Article 47.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-114: Maintain Technical Documentation for Financial Institutions

### Control Objective:

To ensure that providers of high-risk AI systems that are financial institutions maintain technical documentation as part of their existing documentation under Union financial services law.

### Implementation Guidance:

1. Maintain technical documentation as part of the documentation kept under relevant Union financial services law.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 18, Section 3: Providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the technical documentation as part of the documentation kept under the relevant Union financial services law.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 Obligations of providers and deployers of high-risk AI systems and other parties, Article 19 Automatically generated logs

### Automatically Generated Logs

*To ensure that providers of high-risk AI systems maintain logs generated by their systems for a specified period, contributing to transparency and accountability.*

#### AIAct-115: Maintain Automatically Generated Logs

##### Control Objective:

To ensure that providers of high-risk AI systems maintain logs generated by their systems for a specified period.

##### Implementation Guidance:

1. Implement a system to automatically generate logs from high-risk AI systems.
2. Ensure logs are retained for a period appropriate to the intended purpose of the AI system, at least six months, unless otherwise specified by applicable Union or national law.
3. Securely store and manage logs to prevent unauthorized access, modification, or deletion.
4. Establish procedures for accessing and reviewing logs for auditing and troubleshooting purposes.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 19(1): Providers of high-risk AI systems shall keep the logs referred to in Article 12(1), automatically generated by their high-risk AI systems, to the extent such logs are under their control. Without prejudice to applicable Union or national law, the logs shall be kept for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in the applicable Union or national law, in particular in Union law on the protection of personal data.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

DRAFT



## AIAct-116: Maintain Logs for Financial Institutions

### Control Objective:

To ensure that financial institutions maintain logs generated by their high-risk AI systems as part of their documentation.

### Implementation Guidance:

1. Integrate log generation and retention into existing documentation practices for financial institutions.
2. Ensure logs are maintained in accordance with relevant financial services law.
3. Establish clear procedures for accessing and reviewing logs for regulatory compliance and internal audits.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 19(2): Providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the logs automatically generated by their high-risk AI systems as part of the documentation kept under the relevant financial services law.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 Obligations of providers and deployers of high-risk AI systems and other parties, Article 21 Cooperation with competent authorities

### Cooperation with Competent Authorities

*To establish a framework for cooperation between providers of high-risk AI systems and competent authorities to ensure compliance with the regulation.*

#### AIAct-119: Provide Information and Documentation to Competent Authorities

##### Control Objective:

To ensure that providers of high-risk AI systems can provide all necessary information and documentation to demonstrate conformity with the regulation upon request from a competent authority.

##### Implementation Guidance:

1. Establish a process for receiving and responding to reasoned requests from competent authorities.
2. Maintain comprehensive documentation demonstrating the conformity of the high-risk AI system with the requirements set out in Section 2.
3. Ensure that documentation is readily available in a language easily understood by the authority.
4. Train personnel on the requirements of the regulation and the process for responding to requests from competent authorities.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 21, Section 1: Providers of high-risk AI systems shall, upon a reasoned request by a competent authority, provide that authority all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements set out in Section

2, in a language which can be easily understood by the authority in one of the official languages of the institutions of the Union as indicated by the Member State concerned.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

DRAFT

## AIAct-120: Provide Access to AI System Logs

### Control Objective:

To ensure that providers of high-risk AI systems can provide access to automatically generated logs upon request from a competent authority.

### Implementation Guidance:

1. Establish a process for receiving and responding to reasoned requests from competent authorities for access to logs.
2. Ensure that logs are securely stored and readily accessible.
3. Implement appropriate access controls to ensure that only authorized personnel can access logs.
4. Train personnel on the requirements of the regulation and the process for providing access to logs.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 21, Section 2: Upon a reasoned request by a competent authority, providers shall also give the requesting competent authority, as applicable, access to the automatically generated logs of the high-risk AI system referred to in Article 12(1), to the extent such logs are under their control.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 Obligations of providers and deployers of high-risk AI systems and other parties, Article 25 Responsibilities along the AI value chain

### Responsibilities along the AI value chain

*To clarify the responsibilities of various actors involved in the AI value chain, particularly for high-risk AI systems.*

#### AIAct-146: Compliance with Provider Obligations for High-Risk AI Systems

##### Control Objective:

To ensure that distributors, importers, deployers, and third-parties comply with the obligations of a provider for high-risk AI systems under Article 16.

##### Implementation Guidance:

1. Conduct a thorough assessment to determine if the AI system falls under the definition of a high-risk AI system.
2. Implement appropriate controls to ensure compliance with the obligations outlined in Article 16, including but not limited to risk assessment, documentation, transparency, and post-market monitoring.
3. Maintain clear and accurate records of all activities related to the AI system, including modifications, intended purpose changes, and any third-party involvement.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 25, Paragraph 1: Any distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-147: Brand Association with High-Risk AI Systems

### Control Objective:

To ensure that companies placing their name or trademark on a high-risk AI system comply with the provider obligations under Article 16.

### Implementation Guidance:

1. Conduct a thorough due diligence process before associating their brand with a high-risk AI system.
2. Ensure that the AI system meets all the requirements outlined in Article 16, including risk assessment, documentation, transparency, and post-market monitoring.
3. Establish clear contractual arrangements with the original provider to allocate responsibilities and ensure compliance with the regulation.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 1(a): they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-148: Substantial Modification of High-Risk AI Systems

### Control Objective:

To ensure that companies making substantial modifications to high-risk AI systems comply with the provider obligations under Article 16.

### Implementation Guidance:

1. Establish a clear process for identifying and assessing substantial modifications to high-risk AI systems.
2. Conduct a thorough risk assessment to determine if the modification maintains the AI system as high-risk under Article 6.
3. Ensure that the modified AI system meets all the requirements outlined in Article 16, including risk assessment, documentation, transparency, and post-market monitoring.
4. Maintain detailed records of all modifications made to the AI system.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 1(b): they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system pursuant to Article 6;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-149: Modification of Intended Purpose for High-Risk AI Systems

### Control Objective:

To ensure that companies modifying the intended purpose of an AI system, resulting in it becoming a high-risk AI system, comply with the provider obligations under Article 16.

### Implementation Guidance:

1. Establish a clear process for identifying and assessing changes to the intended purpose of AI systems.
2. Conduct a thorough risk assessment to determine if the modified AI system becomes a high-risk AI system under Article 6.
3. Ensure that the modified AI system meets all the requirements outlined in Article 16, including risk assessment, documentation, transparency, and post-market monitoring.
4. Maintain detailed records of all changes made to the intended purpose of the AI system.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 1(c): they modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system in accordance with Article 6.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-150: Cooperation and Information Sharing for High-Risk AI Systems

### Control Objective:

To ensure that initial providers of high-risk AI systems cooperate with new providers and provide necessary information and assistance.

### Implementation Guidance:

1. Establish clear communication channels and procedures for cooperation with new providers.
2. Provide the necessary information and technical access to new providers to ensure compliance with the obligations outlined in the regulation.
3. Offer reasonable assistance to new providers in fulfilling their obligations, particularly regarding conformity assessment.
4. Maintain clear documentation specifying the intended purpose of the AI system and any restrictions on modifications.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 2: Where the circumstances referred to in paragraph 1 occur, the provider that initially placed the AI system on the market or put it into service shall no longer be considered to be a provider of that specific AI system for the purposes of this Regulation. That initial provider shall closely cooperate with new providers and shall make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems. This paragraph shall not apply in cases where the initial provider has clearly specified that its AI system is not to be changed into a high-risk AI system and therefore does not fall under the obligation to hand over the documentation.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-151: Product Manufacturer Responsibility for High-Risk AI Systems

### Control Objective:

To ensure that product manufacturers comply with the provider obligations under Article 16 for high-risk AI systems that are safety components of their products.

### Implementation Guidance:

1. Conduct a thorough assessment to determine if the AI system is a safety component of their product.
2. Ensure that the AI system meets all the requirements outlined in Article 16, including risk assessment, documentation, transparency, and post-market monitoring.
3. Maintain clear and accurate records of all activities related to the AI system, including its integration into the product.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 3: In the case of high-risk AI systems that are safety components of products covered by the Union harmonisation legislation listed in Section A of Annex I, the product manufacturer shall be considered to be the provider of the high-risk AI system, and shall be subject to the obligations under Article 16 under either of the following circumstances:

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-152: Brand Association with High-Risk AI Systems in Products

### Control Objective:

To ensure that product manufacturers comply with the provider obligations under Article 16 when placing a high-risk AI system on the market together with their product.

### Implementation Guidance:

1. Conduct a thorough due diligence process before associating their brand with a high-risk AI system integrated into their product.
2. Ensure that the AI system meets all the requirements outlined in Article 16, including risk assessment, documentation, transparency, and post-market monitoring.
3. Establish clear contractual arrangements with the AI system provider to allocate responsibilities and ensure compliance with the regulation.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 3(a): the high-risk AI system is placed on the market together with the product under the name or trademark of the product manufacturer;

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-153: Brand Association with High-Risk AI Systems in Products (Post-Market)

### Control Objective:

To ensure that product manufacturers comply with the provider obligations under Article 16 when putting a high-risk AI system into service under their brand after the product has been placed on the market.

### Implementation Guidance:

1. Conduct a thorough due diligence process before associating their brand with a high-risk AI system integrated into their product.
2. Ensure that the AI system meets all the requirements outlined in Article 16, including risk assessment, documentation, transparency, and post-market monitoring.
3. Establish clear contractual arrangements with the AI system provider to allocate responsibilities and ensure compliance with the regulation.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 3(b): the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-154: Collaboration Agreements for High-Risk AI Systems

### Control Objective:

To ensure that providers of high-risk AI systems and third-party suppliers have written agreements specifying information, capabilities, technical access, and assistance.

### Implementation Guidance:

1. Establish clear written agreements with third-party suppliers of AI systems, tools, services, components, or processes used in high-risk AI systems.
2. Specify the necessary information, capabilities, technical access, and other assistance required for the provider to comply with the regulation.
3. Ensure that the agreements are based on the generally acknowledged state of the art.
4. Maintain detailed records of all agreements and related communications.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 4: The provider of a high-risk AI system and the third party that supplies an AI system, tools, services, components, or processes that are used or integrated in a high-risk AI system shall, by written agreement, specify the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order to enable the provider of the high-risk AI system to fully comply with the obligations set out in this Regulation. This paragraph shall not apply to third parties making accessible to the public tools, services, processes, or components, other than general-purpose AI models, under a free and open-source licence.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-155: Protection of Intellectual Property and Confidential Information

### Control Objective:

To ensure that the sharing of information and technical access required for compliance with the regulation does not infringe on intellectual property rights, confidential business information, or trade secrets.

### Implementation Guidance:

1. Establish clear policies and procedures for protecting intellectual property rights, confidential business information, and trade secrets.
2. Ensure that all information sharing and technical access provided to new providers or third-party suppliers is done in accordance with applicable Union and national laws.
3. Implement appropriate safeguards to protect sensitive information, such as non-disclosure agreements, data encryption, and access controls.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 25, Paragraph 5: Paragraphs 2 and 3 are without prejudice to the need to observe and protect intellectual property rights, confidential business information and trade secrets in accordance with Union and national law.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 3 Obligations of providers and deployers of high-risk AI systems and other parties, Article 27 Fundamental rights impact assessment for high-risk AI systems

### Fundamental Rights Impact Assessment for High-Risk AI Systems

*To ensure that deployers of high-risk AI systems conduct a thorough assessment of the potential impact on fundamental rights before deploying such systems.*

#### AIAct-168: Conduct Fundamental Rights Impact Assessment

##### Control Objective:

To ensure that deployers of high-risk AI systems conduct a thorough assessment of the potential impact on fundamental rights before deploying such systems.

##### Implementation Guidance:

1. Identify and categorize all high-risk AI systems that fall under the scope of Article 6(2) and Annex III.
2. Develop a comprehensive process for conducting fundamental rights impact assessments for these systems.
3. Ensure that the assessment process includes the elements outlined in Article 27(1)(a)-(f).
4. Document the assessment process and its findings in a clear and concise manner.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 27(1): 'Prior to deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce.'

DRAFT



## AIAct-169: Document Deployment Processes

### Control Objective:

To ensure that deployers document their processes for using high-risk AI systems in line with their intended purpose.

### Implementation Guidance:

1. Develop a detailed description of the deployer's processes for using the high-risk AI system.
2. Ensure that the description clearly outlines the intended purpose of the system and how it will be used in practice.
3. Regularly review and update the documentation to reflect any changes in the deployment processes.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(1)(a): 'a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-170: Define Deployment Timeline and Frequency

### Control Objective:

To ensure that deployers define the intended duration and frequency of use for each high-risk AI system.

### Implementation Guidance:

1. Specify the intended duration of use for the high-risk AI system.
2. Define the frequency with which the system will be used during the specified period.
3. Ensure that the defined timeline and frequency are aligned with the intended purpose of the system.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(1)(b): 'a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-171: Identify Affected Individuals and Groups

### Control Objective:

To ensure that deployers identify the categories of individuals and groups likely to be affected by the use of the high-risk AI system.

### Implementation Guidance:

1. Conduct a thorough analysis to identify all categories of natural persons and groups that could be potentially affected by the use of the high-risk AI system.
2. Consider the specific context of the system's deployment and the potential impact on different demographics and social groups.
3. Document the identified categories and their potential vulnerabilities.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(1)(c): 'the categories of natural persons and groups likely to be affected by its use in the specific context;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-172: Assess Risks of Harm

### Control Objective:

To ensure that deployers assess the specific risks of harm that could impact the identified individuals and groups.

### Implementation Guidance:

1. Analyze the potential risks of harm associated with the use of the high-risk AI system.
2. Consider the specific vulnerabilities of the identified categories of individuals and groups.
3. Review the information provided by the provider pursuant to Article 13 to identify any potential risks.
4. Document the identified risks and their potential impact on the affected individuals and groups.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(1)(d): 'the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-173: Implement Human Oversight Measures

### Control Objective:

To ensure that deployers implement appropriate human oversight measures for the high-risk AI system.

### Implementation Guidance:

1. Develop and implement a robust human oversight framework for the high-risk AI system.
2. Ensure that the oversight measures are aligned with the instructions for use provided by the provider.
3. Clearly define the roles and responsibilities of human overseers in the deployment process.
4. Document the implemented oversight measures and their effectiveness.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(1)(e): 'a description of the implementation of human oversight measures, according to the instructions for use;'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-174: Develop Risk Mitigation Strategies

### Control Objective:

To ensure that deployers develop and implement measures to mitigate the identified risks of harm.

### Implementation Guidance:

1. Develop and implement specific measures to mitigate the identified risks of harm.
2. Establish clear procedures for responding to incidents and addressing complaints.
3. Ensure that the risk mitigation strategies are aligned with the arrangements for internal governance and complaint mechanisms.
4. Regularly review and update the risk mitigation strategies based on experience and new information.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(1)(f): 'the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-175: Maintain and Update Impact Assessment

### Control Objective:

To ensure that deployers maintain and update the fundamental rights impact assessment throughout the lifecycle of the high-risk AI system.

### Implementation Guidance:

1. Regularly review the fundamental rights impact assessment to ensure its accuracy and relevance.
2. Update the assessment if any of the elements listed in Article 27(1) change or become outdated.
3. Document all updates and revisions to the impact assessment.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(2): 'The obligation laid down in paragraph 1 applies to the first use of the high-risk AI system. The deployer may, in similar cases, rely on previously conducted fundamental rights impact assessments or existing impact assessments carried out by provider. If, during the use of the high-risk AI system, the deployer considers that any of the elements listed in paragraph 1 has changed or is no longer up to date, the deployer shall take the necessary steps to update the information.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-176: Notify Market Surveillance Authority

### Control Objective:

To ensure that deployers notify the market surveillance authority of the results of the fundamental rights impact assessment.

### Implementation Guidance:

1. Submit the completed fundamental rights impact assessment to the market surveillance authority.
2. Use the template provided in Article 27(5) for the notification.
3. Ensure that the notification is submitted in a timely manner.
4. Maintain records of all notifications submitted to the market surveillance authority.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(3): 'Once the assessment referred to in paragraph 1 of this Article has been performed, the deployer shall notify the market surveillance authority of its results, submitting the filled-out template referred to in paragraph 5 of this Article as part of the notification. In the case referred to in Article 46(1), deployers may be exempt from that obligation to notify.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)



## AIAct-177: Integrate Data Protection Impact Assessment

### Control Objective:

To ensure that deployers integrate the fundamental rights impact assessment with existing data protection impact assessments.

### Implementation Guidance:

1. Review the existing data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680.
2. Ensure that the fundamental rights impact assessment complements the data protection impact assessment.
3. Identify any overlaps or gaps between the two assessments and address them accordingly.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 27(4): 'If any of the obligations laid down in this Article is already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER III HIGH-RISK AI SYSTEMS, SECTION 5 Standards, conformity assessment, certificates, registration, Article 40 Harmonised standards and standardisation deliverables

### Harmonised Standards and Standardisation Deliverables

*To establish a framework for harmonised standards and standardisation deliverables for AI systems, ensuring compliance with the requirements of the regulation.*

#### AIAct-178: Conformity with Harmonised Standards

##### Control Objective:

To ensure that high-risk AI systems or general-purpose AI models comply with harmonised standards.

##### Implementation Guidance:

1. Regularly review and update knowledge of published harmonised standards related to AI systems.
2. Implement processes to ensure that AI systems are designed, developed, and deployed in accordance with relevant harmonised standards.
3. Maintain documentation demonstrating compliance with harmonised standards.
4. Conduct internal audits to verify compliance with harmonised standards.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 40, Section 1: 'High-risk AI systems or general-purpose AI models which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the requirements set out in Section 2 of this Chapter or, as applicable, with the obligations set out in of Chapter V, Sections 2 and 3, of this Regulation, to the extent that those standards cover those requirements or obligations.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.

DRAFT

## AIAct-179: Promote Investment and Innovation in AI

### Control Objective:

To contribute to the promotion of investment and innovation in AI.

### Implementation Guidance:

1. Actively participate in standardisation processes related to AI.
2. Seek opportunities to collaborate with other stakeholders in the AI ecosystem to foster innovation.
3. Explore and implement new technologies and approaches to enhance AI development and deployment.
4. Advocate for policies and regulations that support a thriving AI industry.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 40, Section 3: 'The participants in the standardisation process shall seek to promote investment and innovation in AI, including through increasing legal certainty, as well as the competitiveness and growth of the Union market, to contribute to strengthening global cooperation on standardisation and taking into account existing international standards in the field of AI that are consistent with Union values, fundamental rights and interests, and to enhance multi-stakeholder governance ensuring a balanced representation of interests and the effective participation of all relevant stakeholders in accordance with Articles 5, 6, and 7 of Regulation (EU) No 1025/2012.'

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING AND MARKET SURVEILLANCE, SECTION 5 Supervision, investigation, enforcement and monitoring in respect of providers of general-purpose AI models, Article 93 Power to request measures

### Commission Power to Request Measures

*To empower the Commission to request measures from providers of general-purpose AI models to address systemic risks at the Union level.*

#### AIAct-367: Compliance with Obligations in Articles 53 and 54

##### Control Objective:

To ensure that providers of general-purpose AI models comply with the obligations outlined in Articles 53 and 54.

##### Implementation Guidance:

1. Review and understand the obligations outlined in Articles 53 and 54.
2. Implement appropriate measures to ensure compliance with these obligations.
3. Maintain documentation and records demonstrating compliance with Articles 53 and 54.
4. Regularly review and update compliance measures to reflect changes in regulations or business practices.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 93(1)(a): Where necessary and appropriate, the Commission may request providers to take appropriate measures to comply with the obligations set out in Articles 53 and 54.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-368: Implementation of Mitigation Measures for Systemic Risk

### Control Objective:

To ensure that providers of general-purpose AI models implement mitigation measures to address systemic risks identified through the evaluation process.

### Implementation Guidance:

1. Establish a process for monitoring and evaluating the potential for systemic risks associated with the general-purpose AI model.
2. Develop and implement mitigation measures to address identified systemic risks.
3. Regularly review and update mitigation measures based on new information or changes in the risk landscape.
4. Maintain documentation and records of the mitigation measures implemented and their effectiveness.

### Implementation Status:

Yes

No

Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 93(1)(b): implement mitigation measures, where the evaluation carried out in accordance with Article 92 has given rise to serious and substantiated concern of a systemic risk at Union level.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-369: Restriction, Withdrawal, or Recall of General-Purpose AI Models

### Control Objective:

To ensure that providers of general-purpose AI models comply with requests to restrict, withdraw, or recall their models.

### Implementation Guidance:

1. Establish a process for responding to requests from the Commission regarding the restriction, withdrawal, or recall of the model.
2. Develop and implement procedures for restricting, withdrawing, or recalling the model in accordance with Commission directives.
3. Maintain documentation and records of all actions taken in response to requests for restriction, withdrawal, or recall.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 93(1)(c): restrict the making available on the market, withdraw or recall the model.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## CHAPTER XIII FINAL PROVISIONS, Article 111 AI systems already placed on the market or put into service and general-purpose AI models already placed on the market

### AI Systems Already Placed on the Market

*To establish transitional provisions for AI systems already placed on the market or put into service before the effective date of the regulation.*

#### AIAct-372: Compliance with Regulation for Existing AI Systems

##### Control Objective:

To ensure that AI systems already placed on the market or put into service before 2 August 2027 comply with the requirements of the regulation by 31 December 2030.

##### Implementation Guidance:

1. Conduct a comprehensive assessment of AI systems that are components of large-scale IT systems established by the legal acts listed in Annex X to determine their compliance with the requirements of the regulation.
2. Develop and implement a plan to bring non-compliant AI systems into compliance by 31 December 2030.
3. Maintain documentation of the assessment and compliance plan.
4. Regularly monitor the performance and compliance of AI systems to ensure ongoing adherence to the regulation.

##### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

##### AIAct requirement statement:

Article 111(1): Without prejudice to the application of Article 5 as referred to in Article 113(3), point (a), AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex X that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

LinkedIn post has number of pages restriction. Full version download information can be found on the last page.



DRAFT

## AIAct-373: Compliance with Regulation for Existing High-Risk AI Systems

### Control Objective:

To ensure that operators of high-risk AI systems, other than those referred to in paragraph 1, comply with the regulation if the systems undergo significant design changes after 2 August 2026.

### Implementation Guidance:

1. Establish a process to track and monitor significant design changes to high-risk AI systems.
2. Conduct a compliance assessment of high-risk AI systems whenever significant design changes occur.
3. Implement necessary measures to bring the AI system into compliance with the regulation following significant design changes.
4. For high-risk AI systems intended for use by public authorities, ensure compliance with the regulation by 2 August 2030.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 111(2): Without prejudice to the application of Article 5 as referred to in Article 113(3), point (a), this Regulation shall apply to operators of high-risk AI systems, other than the systems referred to in paragraph 1 of this Article, that have been placed on the market or put into service before 2 August 2026, only if, as from that date, those systems are subject to significant changes in their designs. In any case, the providers and deployers of high-risk AI systems intended to be used by public authorities shall take the necessary steps to comply with the requirements and obligations of this Regulation by 2 August 2030.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## AIAct-374: Compliance with Regulation for Existing General-Purpose AI Models

### Control Objective:

To ensure that providers of general-purpose AI models comply with the regulation by 2 August 2027.

### Implementation Guidance:

1. Review the existing general-purpose AI models to identify any areas of non-compliance with the regulation.
2. Develop and implement a plan to bring the AI models into compliance by 2 August 2027.
3. Maintain documentation of the compliance plan and any actions taken to achieve compliance.

### Implementation Status:

- Yes
- No
- Not Applicable. Reason: \_\_\_\_\_

### AIAct requirement statement:

Article 111(3): Providers of general-purpose AI models that have been placed on the market before 2 August 2025 shall take the necessary steps in order to comply with the obligations laid down in this Regulation by 2 August 2027.

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

## END OF DOCUMENT

DRAFT



Thank you for taking the time to review the Controls Checklist document.

We also appreciate any feedback or comments you may have on the document. Your input helps us improve our resources for everyone.

Don't hesitate to visit the GRC Library to explore other resources that can support your GRC activities.

Best regards,

GRC Library: <https://grclibrary.com>

LinkedIn Page: <https://www.linkedin.com/company/grclibrary/>

### **EU AI Act Controls Checklist (Full Version Download Link)**

[https://grclibrary.com/item\\_display.php?id=7d4b3811-9dc4-41e6-8fb5-b5ecf97e9b85](https://grclibrary.com/item_display.php?id=7d4b3811-9dc4-41e6-8fb5-b5ecf97e9b85)