AI HR Technology Compliance Checklist

European Union Jurisdiction

Date:

Author:



**Document Version:**
**Effective Date:**
**Review Cycle:** Annual with quarterly updates for regulatory changes
**Next Review Date:**
**Document Owner:**

**Distribution List:**

* Head of Talent Acquisition - EU
* EU Data Protection Officer
* Legal Counsel - EU AI/Employment Law
* Head of Information Security - EU
* Country HR Directors (Germany, France, Netherlands, others as applicable)
* Vendor Management Lead

**Approval Framework**

**Required Approvals:**

[ ] EU Data Protection Officer

[ ] Legal Counsel - AI and Employment Law

[ ] Head of Information Security

[ ] Head of Talent Acquisition - EU

**Emergency Review Triggers:**

* Major regulatory guidance releases
* Significant penalty enforcement actions
* AI Act implementing act publications
* Member state implementation variations

Table of Contents

[Executive Summary 5](#_Toc209722111)

[Section 1: EU AI Act Compliance Framework 6](#_Toc209722112)

[1.1 High-Risk AI System Classification 6](#_Toc209722113)

[Checkpoint 1.1.1: AI System Risk Classification 6](#_Toc209722114)

[Checkpoint 1.1.2: Conformity Assessment Procedures 6](#_Toc209722115)

[1.2 Provider Obligations (AI System Vendors) 7](#_Toc209722116)

[Checkpoint 1.2.1: Technical and Organizational Requirements 7](#_Toc209722117)

[Checkpoint 1.2.2: Human Oversight and Transparency 7](#_Toc209722118)

[1.3 Deployer Obligations (Client Organizations) 8](#_Toc209722119)

[Checkpoint 1.3.1: Fundamental Rights Impact Assessment (FRIA) 8](#_Toc209722120)

[Checkpoint 1.3.2: Workplace Notification and Consultation 8](#_Toc209722121)

[Section 2: GDPR Integration and Data Protection 10](#_Toc209722122)

[2.1 Article 22 Automated Decision-Making 10](#_Toc209722123)

[Checkpoint 2.1.1: Automated Decision-Making Assessment 10](#_Toc209722124)

[Checkpoint 2.1.2: Enhanced Transparency Requirements 10](#_Toc209722125)

[2.2 Data Protection Impact Assessment (DPIA) 11](#_Toc209722126)

[Checkpoint 2.2.1: Comprehensive DPIA Requirements 11](#_Toc209722127)

[Checkpoint 2.2.2: Cross-Border Transfer Assessment 11](#_Toc209722128)

[Section 3: NIS2 Directive and Cybersecurity 13](#_Toc209722129)

[3.1 Entity Classification and Scope 13](#_Toc209722130)

[Checkpoint 3.1.1: Entity Classification Assessment 13](#_Toc209722131)

[Checkpoint 3.1.2: Cybersecurity Risk Management 13](#_Toc209722132)

[3.2 Management Accountability and Governance 14](#_Toc209722133)

[Checkpoint 3.2.1: Management Responsibilities 14](#_Toc209722134)

[Section 4: Cyber Resilience Act Compliance 15](#_Toc209722135)

[4.1 Product Scope and Essential Requirements 15](#_Toc209722136)

[Checkpoint 4.1.1: Product Classification 15](#_Toc209722137)

[Checkpoint 4.1.2: Security by Design and Lifecycle Management 15](#_Toc209722138)

[Section 5: Member State Employment Law 17](#_Toc209722139)

[5.1 Works Council and Employee Consultation 17](#_Toc209722140)

[Checkpoint 5.1.1: Germany - Works Constitution Act 17](#_Toc209722141)

[Checkpoint 5.1.2: France - Information and Consultation 17](#_Toc209722142)

[Checkpoint 5.1.3: Netherlands - Works Council Requirements 18](#_Toc209722143)

[5.2 Anti-Discrimination and Bias Prevention 18](#_Toc209722144)

[Checkpoint 5.2.1: Statistical Discrimination Testing 18](#_Toc209722145)

[Section 6: Vendor Risk Management and Due Diligence 19](#_Toc209722146)

[6.1 AI Act Provider Assessment 19](#_Toc209722147)

[Checkpoint 6.1.1: Provider Compliance Verification 19](#_Toc209722148)

[Checkpoint 6.1.2: Technical Documentation Review 19](#_Toc209722149)

[6.2 Contractual Risk Allocation 20](#_Toc209722150)

[Checkpoint 6.2.1: Liability and Indemnification Framework 20](#_Toc209722151)

[Checkpoint 6.2.2: Ongoing Compliance and Monitoring 20](#_Toc209722152)

[Section 7: Cross-Border Data Transfer Management 22](#_Toc209722153)

[7.1 Adequacy and Transfer Mechanism Assessment 22](#_Toc209722154)

[Checkpoint 7.1.1: Transfer Mapping and Assessment 22](#_Toc209722155)

[Checkpoint 7.1.2: Third Country Risk Assessment 22](#_Toc209722156)

[Section 8: Implementation Timeline and Milestones 24](#_Toc209722157)

[8.1 Critical EU AI Act Deadlines 24](#_Toc209722158)

[Checkpoint 8.1.1: Immediate Compliance (February 2, 2025) 24](#_Toc209722159)

[Checkpoint 8.1.2: High-Risk System Compliance (August 2, 2026) 24](#_Toc209722160)

[8.2 Ongoing Compliance Monitoring 25](#_Toc209722161)

[Checkpoint 8.2.1: Regulatory Development Tracking 25](#_Toc209722162)

[Section 9: Documentation and Evidence Framework 26](#_Toc209722163)

[9.1 Compliance Documentation Requirements 26](#_Toc209722164)

[Checkpoint 9.1.1: Mandatory Documentation Framework 26](#_Toc209722165)

[Checkpoint 9.1.2: Retention and Access Procedures 26](#_Toc209722166)

[Section 10: Crisis Management and Incident Response 28](#_Toc209722167)

[10.1 AI Incident Response Framework 28](#_Toc209722168)

[Checkpoint 10.1.1: Incident Classification and Response 28](#_Toc209722169)

[Checkpoint 10.1.2: Stakeholder Communication 28](#_Toc209722170)

Executive Summary

This compliance checklist provides EU talent acquisition teams with a comprehensive framework for evaluating AI HR technology solutions in accordance with the EU AI Act, GDPR, NIS2 Directive, and Cyber Resilience Act. The checklist addresses the complex regulatory landscape created by overlapping EU legislation, with particular focus on high-risk AI system obligations and cross-border data protection requirements.

**Critical Context:** The EU AI Act classifies HR AI systems as high-risk under Annex III, creating extensive compliance obligations by August 2, 2026. Penalties reach €35 million or 7% of global turnover for prohibited practices, €15 million or 3% for high-risk violations, and €7.5 million or 1% for information obligations. Combined with GDPR, NIS2, and cybersecurity requirements, total potential exposure exceeds €50 million for comprehensive violations.

**Purpose:** This document enables talent acquisition professionals to assess AI HR technology vendors and internal readiness for EU regulatory compliance. Each checkpoint provides regulatory context, implementation guidance, and risk assessment criteria for informed decision-making across member state operations.

Section 1: EU AI Act Compliance Framework

1.1 High-Risk AI System Classification

**Regulation:** EU AI Act Article 6 and Annex III, Point 4
**Risk Level:** CRITICAL - €15 million or 3% global turnover penalties

Checkpoint 1.1.1: AI System Risk Classification

[ ] **High-Risk Determination:** Confirm AI system falls under Annex III, Point 4 (recruitment/selection or employment decisions)

[ ] **Provider vs. Deployer Status:** Establish organizational role and corresponding obligations

[ ] **CE Marking Requirements:** Verify conformity assessment and marking obligations for providers

[ ] **EU Database Registration:** Confirm registration requirements before market placement

**Objective:** Accurately classify AI systems and determine applicable compliance obligations
**Implementation:** Conduct comprehensive system assessment with legal counsel and technical experts

Checkpoint 1.1.2: Conformity Assessment Procedures

[ ] **Technical Documentation:** Ensure comprehensive system documentation per Annex IV

[ ] **Quality Management System:** Implement ISO 9001-aligned quality processes

[ ] **Risk Management System:** Establish continuous risk identification and mitigation

[ ] **Declaration of Conformity:** Prepare formal compliance declarations for providers

**Objective:** Meet pre-market compliance requirements for high-risk AI systems
**Implementation:** Engage notified bodies for conformity assessment where required

1.2 Provider Obligations (AI System Vendors)

**Regulation:** EU AI Act Articles 16-25
**Risk Level:** HIGH - Direct provider responsibilities with significant penalties

Checkpoint 1.2.1: Technical and Organizational Requirements

[ ] **Risk Management System:** Verify continuous risk assessment and mitigation processes

[ ] **Data Governance:** Confirm training data quality, bias assessment, and validation procedures

[ ] **Technical Documentation:** Review comprehensive system specifications and performance metrics

[ ] **Recordkeeping:** Verify automatic log generation and 10-year retention capabilities

**Objective:** Ensure AI providers meet comprehensive technical obligations
**Implementation:** Conduct detailed vendor due diligence with technical documentation review

Checkpoint 1.2.2: Human Oversight and Transparency

[ ] **Meaningful Human Oversight:** Verify design enables effective human supervision

[ ] **Instructions for Use:** Review comprehensive deployment guidance for deployers

[ ] **Transparency Obligations:** Confirm clear system capability and limitation disclosure

[ ] **Post-Market Monitoring:** Assess ongoing performance monitoring and improvement systems

**Objective:** Ensure AI systems enable effective human oversight and transparent operation
**Implementation:** Test human oversight capabilities and review monitoring procedures

1.3 Deployer Obligations (Client Organizations)

**Regulation:** EU AI Act Articles 26-27
**Risk Level:** CRITICAL - Direct organizational liability for deployment decisions

Checkpoint 1.3.1: Fundamental Rights Impact Assessment (FRIA)

[ ] **Assessment Requirement:** Determine FRIA necessity based on public/private service classification

[ ] **Affected Populations:** Identify and analyze impacted groups and individuals

[ ] **Risk Identification:** Conduct comprehensive fundamental rights risk assessment

[ ] **Mitigation Measures:** Implement appropriate safeguards and monitoring systems

**Objective:** Fulfill mandatory assessment requirements for public bodies and qualifying private entities
**Implementation:** Engage fundamental rights experts and conduct stakeholder consultation

Checkpoint 1.3.2: Workplace Notification and Consultation

[ ] **Worker Information:** Notify employees about high-risk AI system deployment per Article 26

[ ] **Worker Representatives:** Inform trade unions and works councils as applicable

[ ] **Member State Variations:** Address country-specific consultation requirements

[ ] **Documentation Requirements:** Maintain records of notification and consultation processes

**Objective:** Comply with workplace transparency and consultation obligations
**Implementation:** Develop member state-specific notification procedures and templates

Section 2: GDPR Integration and Data Protection

2.1 Article 22 Automated Decision-Making

**Regulation:** GDPR Article 22, EDPB Guidelines WP251
**Risk Level:** CRITICAL - €20 million or 4% global turnover penalties

Checkpoint 2.1.1: Automated Decision-Making Assessment

[ ] **Solely Automated Determination:** Assess whether decisions are made without meaningful human involvement

[ ] **Legal/Similar Effects:** Evaluate impact significance on individuals' legal status or rights

[ ] **Exception Application:** Document reliance on contract necessity, consent, or legal authorization

[ ] **Safeguards Implementation:** Ensure human intervention rights, explanation provision, and contest mechanisms

**Objective:** Prevent GDPR Article 22 violations through proper safeguard implementation
**Implementation:** Conduct detailed decision-making process mapping and safeguard verification

Checkpoint 2.1.2: Enhanced Transparency Requirements

[ ] **Algorithm Information:** Provide meaningful information about automated logic (Articles 13-14)

[ ] **Decision Factors:** Explain main elements considered in automated decisions

[ ] **Human Rights:** Implement access, rectification, erasure, and portability mechanisms

[ ] **Data Minimization:** Ensure processing limited to necessary data for legitimate purposes

**Objective:** Meet enhanced transparency obligations for automated processing systems
**Implementation:** Develop comprehensive privacy notices and data subject response procedures

2.2 Data Protection Impact Assessment (DPIA)

**Regulation:** GDPR Article 35, AI Act Article 27
**Risk Level:** HIGH - Mandatory for high-risk processing with enforcement scrutiny

Checkpoint 2.2.1: Comprehensive DPIA Requirements

* [ ] **Processing Description:** Detail AI system data processing activities and purposes
* [ ] **Necessity Assessment:** Justify processing proportionality and legitimate interest balancing
* [ ] **Risk Analysis:** Identify data protection risks to individuals' rights and freedoms
* [ ] **Mitigation Measures:** Implement technical and organizational safeguards

**Objective:** Fulfill mandatory DPIA requirements for high-risk AI processing
**Implementation:** Engage data protection specialists and conduct stakeholder consultation

Checkpoint 2.2.2: Cross-Border Transfer Assessment

* [ ] **Transfer Mapping:** Identify all international data transfers within AI processing chain
* [ ] **Adequacy Decisions:** Verify adequacy status for destination countries
* [ ] **Appropriate Safeguards:** Implement SCCs, BCRs, or other transfer mechanisms
* [ ] **Transfer Impact Assessment:** Conduct TIA for high-risk transfer scenarios

**Objective:** Ensure lawful international data transfers throughout AI processing lifecycle
**Implementation:** Map complete data flow architecture and implement appropriate transfer safeguards

Section 3: NIS2 Directive and Cybersecurity

3.1 Entity Classification and Scope

**Regulation:** NIS2 Directive (EU) 2022/2555
**Risk Level:** HIGH - €10 million/2% (Essential) or €7 million/1.4% (Important) penalties

Checkpoint 3.1.1: Entity Classification Assessment

[ ] **Size Threshold Analysis:** Determine Essential (≥250 employees or €50M turnover) or Important Entity status

[ ] **Sector Classification:** Assess digital infrastructure or digital service provider categorization

[ ] **Member State Implementation:** Review national transposition status and requirements

[ ] **Supply Chain Impact:** Evaluate upstream and downstream cybersecurity obligations

**Objective:** Accurately determine NIS2 obligations and ensure appropriate compliance measures
**Implementation:** Conduct comprehensive organizational assessment with cybersecurity experts

Checkpoint 3.1.2: Cybersecurity Risk Management

[ ] **Risk Assessment Procedures:** Implement comprehensive cybersecurity risk management

[ ] **Incident Response:** Establish 24-hour incident reporting capabilities to national authorities

[ ] **Business Continuity:** Develop resilience measures for AI system disruptions

[ ] **Supply Chain Security:** Assess and monitor vendor cybersecurity practices per Article 23

**Objective:** Implement comprehensive cybersecurity risk management framework
**Implementation:** Engage cybersecurity consultants and develop incident response procedures

3.2 Management Accountability and Governance

**Regulation:** NIS2 Article 20
**Risk Level:** CRITICAL - Personal management liability for gross negligence

Checkpoint 3.2.1: Management Responsibilities

[ ] **Cybersecurity Governance:** Implement board-level cybersecurity oversight

[ ] **Risk Management Approval:** Ensure management approval of cybersecurity strategies

[ ] **Training Requirements:** Provide cybersecurity awareness training for management

[ ] **Incident Accountability:** Establish clear management responsibilities for breach response

**Objective:** Ensure management fulfills personal cybersecurity accountability obligations
**Implementation:** Develop management cybersecurity governance framework and training programs

Section 4: Cyber Resilience Act Compliance

4.1 Product Scope and Essential Requirements

**Regulation:** Cyber Resilience Act (EU) 2024/2847
**Risk Level:** MEDIUM - Applies to AI software products by December 2027

Checkpoint 4.1.1: Product Classification

[ ] **Digital Element Assessment:** Determine whether AI HR software qualifies as "product with digital elements"

[ ] **Critical Product Classification:** Assess potential classification as critical product requiring enhanced measures

[ ] **CE Marking Requirements:** Verify cybersecurity conformity assessment and marking obligations

[ ] **Market Surveillance:** Prepare for regulatory oversight and compliance verification

**Objective:** Ensure AI software products meet essential cybersecurity requirements
**Implementation:** Conduct product classification assessment and prepare for 2027 compliance

Checkpoint 4.1.2: Security by Design and Lifecycle Management

[ ] **Security by Design:** Verify AI systems incorporate cybersecurity from development stage

[ ] **Vulnerability Handling:** Assess vendor capability for 5-year minimum vulnerability management

[ ] **Software Bill of Materials:** Review SBOM documentation for supply chain transparency

[ ] **Update Mechanisms:** Verify secure software update capabilities and procedures

**Objective:** Ensure AI products meet security by design and lifecycle management requirements
**Implementation:** Review vendor development practices and vulnerability management capabilities

Section 5: Member State Employment Law

5.1 Works Council and Employee Consultation

**Regulations:** National implementations of Directive 2002/14/EC
**Risk Level:** HIGH - Varies by member state with potential operational disruption

Checkpoint 5.1.1: Germany - Works Constitution Act

[ ] **Co-determination Rights:** Assess Section 87(1) No. 6 monitoring system requirements

[ ] **Works Council Consent:** Secure agreement for AI deployment in German operations

[ ] **Data Protection Integration:** Align works council consultation with GDPR requirements

[ ] **Implementation Timeline:** Plan consultation processes before AI system deployment

**Objective:** Ensure compliance with German co-determination requirements
**Implementation:** Engage German employment lawyers and initiate works council consultations

Checkpoint 5.1.2: France - Information and Consultation

[ ] **Social and Economic Committee:** Conduct mandatory consultation on AI implementation

[ ] **Impact Assessment Sharing:** Provide detailed analysis of employment impact

[ ] **Alternative Analysis:** Document consideration of non-AI alternatives

[ ] **Implementation Monitoring:** Establish ongoing consultation during deployment

**Objective:** Fulfill French employee consultation obligations for significant workplace changes
**Implementation:** Engage French employment specialists and develop consultation timeline

Checkpoint 5.1.3: Netherlands - Works Council Requirements

[ ] **Advice Rights:** Secure works council advice on recruitment process changes

[ ] **Corporate Group Consultation:** Address cross-border consultation requirements

[ ] **Appeal Procedures:** Implement works council decision appeal mechanisms

[ ] **Ongoing Monitoring:** Establish continuous consultation for system modifications

**Objective:** Comply with Dutch works council consultation requirements
**Implementation:** Engage Dutch employment lawyers and establish consultation procedures

5.2 Anti-Discrimination and Bias Prevention

**Regulations:** National implementations of Directive 2000/43/EC and 2000/78/EC
**Risk Level:** CRITICAL - Varying national penalties and enforcement approaches

Checkpoint 5.2.1: Statistical Discrimination Testing

[ ] **Protected Characteristics:** Test for bias across all EU-recognized protected grounds

[ ] **Intersectional Analysis:** Assess compound discrimination effects

[ ] **Member State Variations:** Address country-specific protected characteristics

[ ] **Positive Action Assessment:** Evaluate potential positive discrimination measures

**Objective:** Ensure AI systems comply with EU anti-discrimination directives
**Implementation:** Conduct comprehensive bias testing across all member state operations

Section 6: Vendor Risk Management and Due Diligence

6.1 AI Act Provider Assessment

**Requirements:** EU AI Act provider obligation verification
**Risk Level:** CRITICAL - Deployer liability for provider non-compliance

Checkpoint 6.1.1: Provider Compliance Verification

[ ] **CE Marking Verification:** Confirm valid conformity marking and documentation

[ ] **EU Database Registration:** Verify provider registration in mandatory database

[ ] **Instructions for Use:** Review comprehensive deployment guidance and limitations

[ ] **Post-Market Monitoring:** Assess provider ongoing monitoring and improvement systems

**Objective:** Ensure AI providers meet all EU AI Act obligations before deployment
**Implementation:** Conduct comprehensive provider due diligence with technical verification

Checkpoint 6.1.2: Technical Documentation Review

[ ] **Risk Management System:** Review comprehensive risk assessment and mitigation documentation

[ ] **Training Data Assessment:** Evaluate data quality, representativeness, and bias mitigation

[ ] **Performance Metrics:** Assess accuracy, fairness, and robustness testing results

[ ] **Human Oversight Design:** Verify system design enables meaningful human control

**Objective:** Verify AI systems meet technical requirements for safe and effective deployment
**Implementation:** Engage technical experts for comprehensive documentation review

6.2 Contractual Risk Allocation

**Framework:** EU contract law, product liability directives
**Risk Level:** CRITICAL - Multi-million euro penalty exposure requires clear risk allocation

Checkpoint 6.2.1: Liability and Indemnification Framework

[ ] **AI Act Penalty Coverage:** Allocate responsibility for €35 million maximum penalties

[ ] **GDPR Fine Responsibility:** Address €20 million data protection penalty exposure

[ ] **NIS2 Cybersecurity Fines:** Assign €10 million cybersecurity penalty responsibility

[ ] **Member State Variations:** Address country-specific liability and penalty frameworks

**Objective:** Appropriately allocate regulatory penalty risks between parties
**Implementation:** Engage EU contract specialists for comprehensive risk allocation negotiation

Checkpoint 6.2.2: Ongoing Compliance and Monitoring

[ ] **Continuous Compliance Warranties:** Secure ongoing AI Act and GDPR compliance representations

[ ] **Audit Rights:** Establish comprehensive system audit and assessment rights

[ ] **Incident Notification:** Require immediate disclosure of compliance violations or incidents

[ ] **Remediation Obligations:** Define correction timeframes and escalation procedures

**Objective:** Maintain ongoing visibility and control over vendor compliance performance
**Implementation:** Establish vendor governance framework with regular compliance verification

Section 7: Cross-Border Data Transfer Management

7.1 Adequacy and Transfer Mechanism Assessment

**Regulation:** GDPR Chapter V, EDPB Recommendations
**Risk Level:** HIGH - €20 million penalty exposure for unlawful transfers

Checkpoint 7.1.1: Transfer Mapping and Assessment

[ ] **Complete Data Flow Mapping:** Document all international transfers in AI processing chain

[ ] **Adequacy Decision Status:** Verify current adequacy status for all destination countries

[ ] **Transfer Impact Assessment:** Conduct TIA for transfers to countries without adequacy decisions

[ ] **Appropriate Safeguards:** Implement SCCs, BCRs, or alternative transfer mechanisms

**Objective:** Ensure all international data transfers comply with GDPR requirements
**Implementation:** Conduct comprehensive data mapping and implement appropriate transfer safeguards

Checkpoint 7.1.2: Third Country Risk Assessment

[ ] **Government Access Laws:** Assess destination country surveillance and data access laws

[ ] **Judicial Redress:** Evaluate available legal remedies for data subjects

[ ] **Additional Safeguards:** Implement supplementary measures for high-risk transfers

[ ] **Ongoing Monitoring:** Establish continuous monitoring of third country legal developments

**Objective:** Mitigate risks associated with transfers to countries without adequate protection
**Implementation:** Engage international data protection specialists for risk assessment

Section 8: Implementation Timeline and Milestones

8.1 Critical EU AI Act Deadlines

**Regulation:** EU AI Act Implementation Timeline
**Risk Level:** CRITICAL - Missed deadlines result in immediate penalty exposure

Checkpoint 8.1.1: Immediate Compliance (February 2, 2025)

[ ] **Prohibited AI Systems:** Ensure no use of emotion recognition or similar prohibited systems

[ ] **AI Literacy Programs:** Implement mandatory staff training on AI systems and risks

[ ] **Governance Structure:** Establish AI governance committees and responsible persons

[ ] **Documentation Framework:** Begin comprehensive compliance documentation systems

**Objective:** Meet initial AI Act requirements effective February 2025
**Implementation:** Conduct immediate compliance gap analysis and remediation

Checkpoint 8.1.2: High-Risk System Compliance (August 2, 2026)

[ ] **Conformity Assessment:** Complete full conformity assessment procedures

[ ] **Technical Documentation:** Finalize comprehensive technical documentation packages

[ ] **EU Database Registration:** Complete mandatory database registration before deployment

[ ] **Deployer Obligations:** Implement full FRIA and notification requirements

**Objective:** Achieve full high-risk AI system compliance before mandatory deadline
**Implementation:** Develop detailed compliance project plan with interim milestones

8.2 Ongoing Compliance Monitoring

**Requirements:** Continuous regulatory change monitoring
**Risk Level:** MEDIUM - Regulatory landscape continues evolving rapidly

Checkpoint 8.2.1: Regulatory Development Tracking

[ ] **European Commission Guidance:** Monitor implementing acts and technical standards

[ ] **Member State Implementation:** Track national law transposition and variations

[ ] **EDPB Guidelines:** Follow data protection authority guidance development

[ ] **Case Law Development:** Monitor CJEU and national court decisions

**Objective:** Maintain current awareness of regulatory developments and requirements
**Implementation:** Establish regulatory monitoring framework with legal counsel support

Section 9: Documentation and Evidence Framework

9.1 Compliance Documentation Requirements

**Standards:** EU AI Act Article 12, GDPR accountability principle
**Risk Level:** HIGH - Inadequate documentation prevents compliance demonstration

Checkpoint 9.1.1: Mandatory Documentation Framework

[ ] **AI Act Technical Documentation:** Maintain comprehensive Annex IV documentation

[ ] **GDPR Processing Records:** Document all personal data processing activities (Article 30)

[ ] **Risk Assessment Records:** Maintain current DPIA, FRIA, and risk management documentation

[ ] **Decision Audit Trails:** Log all AI system outputs and human oversight activities

**Objective:** Maintain comprehensive compliance documentation for regulatory verification
**Implementation:** Establish centralized compliance documentation management system

Checkpoint 9.1.2: Retention and Access Procedures

[ ] **10-Year Retention:** Implement AI Act-compliant documentation retention systems

[ ] **Regulatory Access:** Prepare for market surveillance authority inspection requests

[ ] **Data Subject Access:** Enable efficient response to individual information requests

[ ] **Audit Trail Integrity:** Ensure documentation accuracy and modification tracking

**Objective:** Ensure documentation accessibility and integrity for compliance verification
**Implementation:** Implement secure documentation management with appropriate access controls

Section 10: Crisis Management and Incident Response

10.1 AI Incident Response Framework

**Requirements:** AI Act post-market monitoring, NIS2 incident reporting
**Risk Level:** HIGH - Rapid response required for regulatory notification

Checkpoint 10.1.1: Incident Classification and Response

[ ] **Bias Incident Procedures:** Establish detection and response procedures for discrimination incidents

[ ] **System Failure Management:** Implement business continuity measures for AI system failures

[ ] **Data Breach Integration:** Coordinate AI incidents with GDPR breach notification requirements

[ ] **Regulatory Notification:** Prepare for mandatory incident reporting to multiple authorities

**Objective:** Ensure rapid and appropriate response to AI-related incidents
**Implementation:** Develop AI-specific incident response procedures integrated with existing frameworks

Checkpoint 10.1.2: Stakeholder Communication

[ ] **Internal Escalation:** Define management and board notification procedures

[ ] **Regulatory Communication:** Prepare templates for authority notification requirements

[ ] **Affected Individual Notice:** Implement data subject notification procedures

[ ] **Public Relations Management:** Develop crisis communication strategies for reputation protection

**Objective:** Ensure appropriate stakeholder communication during AI incidents
**Implementation:** Develop comprehensive incident communication framework and templates

**CONFIDENTIAL - EU TALENT ACQUISITION TEAM USE ONLY**