EU AI Act Compliance Checklist

Scope, prohibited practices, risk classification, role, deployer duties, transparency and incident obligations, system by system

EU AI Act · ISO/IEC 42001 · GDPR · POPIA

The EU AI Act regulates each AI system on its own terms. What you owe depends on what the system does, where its output is used and whether you are its provider or its deployer. Work through this checklist once per AI system, and again whenever one changes.

A Inventory & Scope

- ☐ Every AI system in use is listed, including tools bought in, built in house and AI features switched on inside existing software
- ☐ Each system has a named business owner and a written description of its intended purpose
- ☐ For each system, you have recorded whether it is placed on the EU market or its output is used in the EU
- ☐ Systems used only for scientific research, personal non-professional use or military purposes are recorded as out of scope, with the reason

B Prohibited Practices & AI Literacy

- ☐ Each system has been checked against the Article 5 prohibited practices before any other assessment
- ☐ Systems that manipulate behaviour, exploit vulnerabilities, perform social scoring or infer emotions in the workplace or education are identified and stopped
- ☐ The check result is recorded with the person who made it and the date
- ☐ Staff who operate or use AI systems have AI literacy training suited to their role (Article 4), with records kept

C Risk Classification

- ☐ Each system is assessed against Annex III use areas, such as employment, credit, education, essential services and law enforcement
- ☐ Systems that are safety components of products covered by Annex I legislation are identified
- ☐ Where an Annex III system is claimed not to be high risk, the Article 6(3) reasoning is documented
- ☐ The final tier (high risk, transparency obligations only or minimal risk) is approved, locked and versioned
- ☐ Classification is repeated when the purpose, capability or users of a system change

D Your Role

- [ ] Your role is recorded per system: provider, deployer, importer or distributor
- [ ] You have checked whether putting your name or trademark on a high-risk system makes you its provider
- [ ] Substantial modifications and changes to intended purpose are reviewed for whether they move provider duties to you (Article 25)
- [ ] Contracts with AI suppliers give you the instructions for use, information and support you need to meet deployer duties

E Deployer Duties for High-Risk Systems

- [ ] The system is used in line with the provider's instructions for use, with technical and organisational measures in place
- [ ] Human oversight is assigned to named people with the competence, training and authority to intervene
- [ ] Input data under your control is relevant and sufficiently representative for the intended purpose
- [ ] Operation is monitored, the provider is informed when the system presents a risk, and automatically generated logs under your control are kept for at least six months
- [ ] Workers and their representatives are told before a high-risk system is used in the workplace

F Rights Impact & Data Protection

- [ ] You have checked whether a fundamental rights impact assessment is required (Article 27), for example for public bodies, public service providers, credit scoring and life or health insurance pricing
- [ ] Where required, the assessment records affected groups, specific risks of harm, oversight measures and complaint routes
- [ ] People subject to decisions made or assisted by a high-risk system are told that it is used
- [ ] A data protection impact assessment under GDPR or a POPIA assessment is completed where personal data is processed

G Transparency Obligations

- [ ] People are told when they are interacting with an AI system such as a chatbot, unless it is obvious
- [ ] AI-generated audio, image, video and text output is marked as artificially generated where the Act requires it
- [ ] Deepfake content you publish is disclosed as artificially generated or manipulated
- [ ] People exposed to emotion recognition or biometric categorisation systems are informed

H Serious Incidents & Change

- [ ] Serious incidents involving a high-risk system are reported to the provider straight away, and onward as the Act requires
- [ ] Providers have a process to report serious incidents to the market surveillance authority within the Article 73 deadlines
- [ ] Incidents are linked to the AI system, its classification and its risks, with root cause and actions recorded
- [ ] Every change to a model, data source, capability or purpose is assessed for re-classification before it goes live
- [ ] Classification, evidence and decisions are retained so you can show what was decided, when and why

© XGRC® Software, a Strategix product. Strategix Application Solutions (Pty) Ltd, Reg No. 2015/192960/07. ISO 27001:2022 certified. info@xgrcsoftware.com