

AI Impact Assessment & DPIA Crosswalk for Regulated Organisations



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval.
NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Describe the system, intended use, affected people and operator roles.
2. Screen DPIA, FRIA and sector duties separately against the applicable law.
3. Share factual evidence without merging distinct assessment conclusions.

A practical architecture for identifying when privacy, fundamental-rights, safety and wider AI governance assessments intersect—and where they must remain separate

Executive proposition: There is no single universal “AI compliance assessment”. A defensible project distinguishes the UK/EU data protection impact assessment (DPIA), any applicable EU AI Act fundamental-rights impact assessment (FRIA), sector safety assessments and the organisation's broader AI risk review, then connects their evidence and decisions without treating one as a substitute for another.

For: Chief AI Officers, AI product leaders, privacy counsel, DPOs, clinical safety leaders, CROs, procurement teams, risk committees and technology owners. **Scope:** assessment design and governance, not a formal legal determination that a specific AI system is high-risk under the EU AI Act.

Executive briefing — the assessment problem

Consider a UK hospital piloting an AI-enabled clinical prioritisation tool supplied by an overseas software provider. Possible workstreams include processing personal or special-category data, patient safety, clinical workflow risk, supplier governance, bias and human oversight, EU AI Act applicability where EU territorial links exist, and information security. Running one generic “AI ethics checklist” will not establish whether each distinct applicable obligation has been satisfied.

An organisation should identify **each assessment's legal or governance basis, the system and operator covered, when it must be conducted, who makes the decision, what evidence is required and when it must be updated**. The assessments can share a factual inventory but not interchangeable legal conclusions.

The ICO requires DPIAs under the UK GDPR where processing is likely to result in a high risk to individuals; AI use is not automatically a DPIA trigger in every context, but many AI applications create relevant high-risk indicators. [S1][S2]

Under Article 27 of the EU AI Act, a FRIA is required **for specified deployers and specified high-risk systems**, not every system and not every organisation using AI. **Timing matters:** the current Commission timeline reports a planning date for relevant Annex III high-risk requirements of **2 December 2027**, not automatically from August 2026. Screen future deployments now, but do not describe a future-applying duty as already operative. Verify the role, category, transitions and any later amendments. [S3][S4]

1. Four assessment instruments with different purposes

Instrument	Principal object	Trigger	Primary decision owner	Not a substitute for
UK/EU GDPR DPIA	High-risk personal-data processing	Article 35 relevant high-risk processing	Controller with DPO advice where appointed	Broader AI safety, ethics or all EU AI Act duties
EU AI Act FRIA	Fundamental-rights impact for specified high-risk deployments	Article 27 where applicable	Relevant deployer	DPIA, provider high-risk conformity assessment
AI governance/impact assessment	Wider safety, robustness, fairness, accountability and operational consequences	Organisation policy, buyer/contract, standards or statutory overlay	Responsible AI governance owner	Mandatory DPIA/FRIA or specialised regulated assessment
Sector-specific safety/risk assessment	Harm in a defined regulated context (e.g. clinical safety)	Sector standards/law and actual intended use	Qualified accountable professional and organisation	Data protection or general AI governance alone

The table states broad conceptual boundaries, not a complete regulatory applicability opinion. ISO/IEC 42001 can support management-system governance without replacing statutory EU AI Act processes, GDPR DPIAs, certification or clinical safety work.

2. The IG-Smart Multi-Assessment Decision Crosswalk – eight gates

Gate	Practitioner question	Reusable evidence	Distinct decisions
A1 System identity	What model, AI system, version and use are being assessed?	System record, intended use, architecture	System boundary and change control
A2 Operators	Who provides, deploys, controls processing and makes decisions?	Entity, operator and controller/processor map	Legal role determination
A3 People and effects	Who may be affected, including vulnerable groups?	Population and impact mapping	Rights, safety and fairness prioritisation
A4 Applicable instruments	What triggers a DPIA, FRIA or sector assessment?	Documented legal tests	Independent trigger conclusions
A5 Risk pathways	What harms can arise, how and with what uncertainty?	Hazard and risk scenarios	Assessment-specific methodology
A6 Safeguards	What measures meaningfully reduce each exposure?	Human oversight, data governance, tests	Control acceptance per domain
A7 Authority	Who may authorise residual exposure or stop deployment?	DPO advice, safety sign-off, board delegation	Separate formal decisions
A8 Lifecycle	What change causes re-evaluation?	Monitoring and incident triggers	Update each affected assessment

Stop condition: if an applicable mandatory assessment is missing, a positive generic AI risk score cannot be treated as authorisation to deploy. Every conclusion must be made by an appropriately accountable person.

3. Begin with a single factual system dossier

A reusable factual inventory avoids duplicated work. Record the system version, provider, deployer, data-controller roles, purpose, use environment, affected populations, intended and reasonably foreseeable use, training and inference data, output and decision pathways, human override, outsourced model dependencies, monitoring and known limitations. Distinguish **facts observed**, **supplier assertions**, **tested findings**, **inferences**, and **unresolved unknowns**.

The same system diagram may be shared among a DPIA, FRIA and clinical safety analysis, but the conclusions must still be specific to the relevant rights, individuals, patient harms or sector requirements.

4. DPIA: privacy-specific obligations and evidence

Screen whether the processing is likely to result in high risk to individuals; map purposes, necessity and proportionality, data flows, categories, lawful basis and any Article 9 condition, fairness and transparency, individual rights, automated decision-making implications, processor responsibilities, retention, security and residual risk. Seek DPO advice where a DPO is appointed and consult the ICO where required by the relevant statutory test for unmitigated high risk.

For an AI-enabled recruitment ranking tool, the DPIA should not simply record that a model is “accurate”. It needs evidence about personal-data use, fairness, explainability where relevant, sensitive inference, candidates' rights and governance of significantly affecting decisions. UK automated decision-making rules require current legal verification following the Data (Use and Access) Act 2025; do not reuse superseded Article 22 summaries as fixed universal rules.

DPIA working fields

Question	Required practical record
Purpose and lawful basis	Legal rationale tied to the actual processing
Data flows	Collection, features, output, access and onward recipients
Affected individuals	Categories and plausible material/non-material harms
Necessity	Why less intrusive alternatives cannot meet the aim
Controls	Measures demonstrably effective in this workflow
Advice and consultation	DPO, affected groups, regulator as appropriate
Residual exposure	Risk after controls, with independent challenge
Decision and review	Controller authority and material change triggers

5. FRIA: fundamental-rights assessment where Article 27 applies

Check the **relevant deployer type**, **high-risk system category**, **exemptions**, **scope and effective application date**. An FRIA must not be claimed necessary for every UK company that purchases generative AI. Where Article 27 applies, the record should consider the proposed use, groups likely affected, duration and frequency, specific fundamental-rights risks, human oversight and response/mitigation arrangements, following the operative law and current official guidance. [S3]

EU fundamental rights may include non-discrimination, privacy, data protection and other context-specific protections; they cannot be collapsed into “GDPR compliant”. A DPIA and FRIA can share factual evidence, but each requires its own statutory test and adequate coverage.

Practical illustration

A public-sector EU deployer proposes a high-risk AI system to prioritise essential benefits. The privacy assessment covers personal-data lawfulness, transparency and risks; the FRIA considers the wider impact on fundamental rights, access to the service, vulnerable groups, oversight and complaint pathways. The role and scope tests determine which duties actually apply. Neither assessment should silently treat another's “low risk” result as binding.

An Article 27 scope check, not a blanket rule. Current Commission Article 27 guidance describes the following scope; verify operative law and transitions: the FRIA requirement concerns specified deployers of Article 6(2) high-risk systems: public-law bodies, private entities providing public services, and deployers of the Annex III point 5(b) creditworthiness/credit-scoring and 5(c) life/health-insurance systems. Annex III point 2 is excluded. Check the exact system category, applicable date and any exceptions. The Article 27 duty is not a general requirement for all UK organisations using AI. [S3]

Where it applies, the assessment has its own content and notification requirements. Relevant material may be reused or cross-referenced from a DPIA, but a privacy assessment alone does not establish that the wider fundamental-rights assessment has been completed. [S3]

6. Additional AI risk and safety domains

Dimension	Example assessment question	Evidence candidate
Model performance	Does performance hold for intended populations?	Validation report and cohort analysis
Data quality	Is input data complete, representative and fit for purpose?	Lineage, bias tests, data validation
Fairness	Could decisions disadvantage protected or vulnerable groups?	Outcome analysis and mitigation choices
Human oversight	Can a competent user detect, challenge and override failure?	Workflow observation and trained-user test
Transparency	Do affected persons understand material AI involvement where required?	Notices and explanation artefacts
Cyber and integrity	Can outputs be manipulated, exfiltrated or tampered with?	Threat assessment and security testing
Clinical/physical safety	Could a wrong recommendation cause patient or physical harm?	Hazard analysis and safety case
Third-party concentration	Can model or API changes invalidate controls?	Contract, change notice and dependency testing
Monitoring	Who detects drift or post-deployment harm?	Thresholds, complaints, incident and review records

A single “red/amber/green” matrix across these fields may be useful for portfolio triage but must not imply that harms of different kinds are commensurable or legally acceptable on a common numeric scale.

7. Independence and conflict-of-interest guardrails

AI suppliers can provide technical documentation, but the deploying organisation must exercise appropriate judgement over its own use. A consultancy implementing a model can help gather evidence, but an independent audit must assess self-review risks. A DPO may advise and monitor DPIAs but does not automatically become the controller's authorising official. Clinical safety decisions require suitably qualified clinical accountability.

An effective governance model records **who designs, who operates, who challenges, who accepts residual risk and who can stop the system**. Unresolved conflict should be escalated rather than concealed behind a shared tool.

8. Six illustrative applications – fictional scenarios

1. **HR applicant ranking:** privacy, fairness, potentially high-risk EU classification where applicable; check role, jurisdiction and automated decision effects.
2. **Clinical decision support:** privacy and local clinical safety assessments, product controls and EU regulatory status where applicable.
3. **Internal code assistant:** intellectual property, security, staff monitoring and supplier risk; avoid assuming every use triggers FRIA.
4. **Insurance pricing model:** profile individual impact, discrimination, transparent governance and sector-specific rules; examine exact EU AI Act classification.
5. **Public-service triage:** assess legal applicability, vulnerable populations, oversight, complaints and evidence of public benefit.
6. **Supplier-provided generative chatbot:** assess disclosed purposes, data retention and secondary training, hallucinations, prompts and incident pathways.

These examples illustrate the assessment questions, not that any described organisation is currently non-compliant.

9. The board decision dossier

System and version: __; **proposed use and affected groups:** __; **operator roles:** __; **territorial applicability:** __; **DPIA screening:** __; **FRIA screening:** __; **sector assessment:** __; **controls evidenced:** __; **open high-consequence risks:** __; **consultations and qualified reviews:** __; **decision options:** proceed / conditional / defer / prohibit; **owner and authority:** __; **monitoring and review trigger:** __.

A final approval should not overwrite a technical or clinical objection. Record dissent, uncertainty and conditions explicitly.

10. Fifteen questions a buyer should ask the AI supplier

- Which exact model and version does your evidence cover?
- Can we inspect intended use and limitations?
- Are you a provider, deployer, GPAI-model provider or another relevant actor?
- Does your training or inference use our data for another purpose?
- How are sensitive, inferred and proxy features evaluated?
- What are the critical error modes and affected populations?
- How have you tested performance outside the development population?
- Can users contest or override consequential outputs?

- What meaningful monitoring detects harmful drift?
- Which safeguards are product-level and which must be deployed locally?
- What EU AI Act classification and evidence claims are actually supported?
- What GDPR assessments have you completed and what remains ours?
- Can material model changes occur without our approval?
- What happens when a serious incident occurs?
- Which claims rely on certification, and what is its actual scope?

11. Frequent questions

Does ISO/IEC 42001 certification replace a DPIA or FRIA? No. Management-system certification and statutory assessments have different tests and scopes.

Must every AI project have a DPIA? Only where the relevant legal high-risk test is met; document screening and apply the law to actual processing.

Must every EU high-risk deployment have an FRIA? Article 27 has specified deployer and system scope; assess the operative text and exceptions.

Are safety and privacy the same risk? No. Harm pathways may overlap but assessment criteria and accountability differ.

Can one evidence register support several reviews? Yes, if provenance and limitations are preserved and each separate decision is adequately supported.

Can a vendor guarantee AI Act compliance for a buyer? Contractual evidence can help, but deployer-specific legal and operational responsibilities remain.

12. Putting the assessment into practice

Next step: Talk to a Senior Practitioner about an actual system, operator model, affected population and assessment scope.

Sources

- [S1] ICO, When do we need to do a DPIA? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/>
- [S2] ICO, Accountability and governance implications of AI <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai>
- [S3] European Commission AI Act Service Desk, Article 27: Fundamental rights impact assessment; guidance checked for the current candidate. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-27>
- [S4] European Commission AI Act Service Desk, Implementation timeline, including the 2026 Digital Omnibus amendments. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/eu-ai-act-implementation-timeline>