TECH ignite

simmons + simmons

Session 1

Designing Compliant Agentic AI – Key Legal Issues for Companies.

Dr Tina Gausling, LL.M. (Columbia University)
Counsel (Munich), Digital Business
Simmons & Simmons Germany

Andrew Joint
Partner (London), Digital Business
Simmons & Simmons

What are AI Agents

New dimension of autonomy

Working definition: An AI agent is a system that perceives its environment, makes decisions, and takes actions autonomously to achieve **goals** – often using reasoning, memory, and external tools.

BEFORE
Generative AI – produce content

- **Reactive, single-step:** input produces output in one cycle
- **Human-in-the-loop: Human decides** how to use the output – AI remains a tool
- **Limited external reach:** typically no access to third-party systems
- **Examples:** ChatGPT conversations, Copilot suggestions

NOW
Agentic AI – acts autonomously

- **Core loop + layers**: perceive-decide-act, with planning, tools, and memory (often LLM-orchestrated)
- **Tools:** APIs, RAG systems, browsers; advanced agents can control software via UI automation (sometimes termed "**LAMs**")
- **Risk profile = tools × autonomy**
  Examples: Claude Code, claims-handling agent, recruiting agent

AUTONOMY GRADES
The legally decisive triad

- **HITL: Human in the Loop:** every action requires user approval
- **HOTL: Human on the Loop:** human supervises and can intervene **before** execution
- **HOOTL: Human out of the Loop:** no prior approval or control

Trade-off: more autonomy = higher productivity, but stricter duties (e.g. Art. 14(2) AI Act)

Consequence: AI agents can act autonomously, but legal responsibility remains with the deploying company (as controller under GDPR) and/or provider and deployer under the AI Act.

Why Agentic AI now: four economic drivers

Avoidance is no longer a realistic compliance strategy

Economic Driver	Mechanism	Hard data points[1]
Knowledge-work productivity	Agents take over **multi-step routine processes** in various, decision inheriting activities, humans become supervisors and escalation points	**$2.6-4.4 trillion** annual value potential of generative and agentic AI across 63 use cases
Scale without headcount	Agentic automation runs **24/7 and in parallel**; absorbs load peaks without additional staff – structural change to the operating model	**60-80 % of routine infrastructure work** automatable; **20-40 % run-rate cost reduction** in early productive deployments
Decision and response speed	Agents reduce **time-to-decision** in regulated and customer-critical processes; from days to minutes in claims, credit, security incidents	**+45 % customer satisfaction** in agent-based service; AI high performers scale agents **3x more often**
Competitive, first-mover pressure	Early adopters set **new service standards**; abstaining is short-term viable but long-term erodes market position	**62 % of companies experimenting** with agents, **23 % scaling** productively

» **Bottom line:** The question is not **whether**, but **how compliantly** agentic AI is deployed – and how early Legal is involved in use-case selection.

1 McKinsey, The State of AI 2025; Seizing the agentic AI advantage

Legal Interfaces of Agentic AI

Focus: GDPR and AI Act

GDPR

GDPR (Regulation (EU) 2016/679)
In force since May 25, 2018

Technology-neutral – captures AI **indirectly** through any processing of personal data

Principles-based: lawfulness, purpose limitation, data minimization, transparency, accountability

Penalties: up to €20m or 4 % global turnover

Practically unavoidable: every productive enterprise agent processes personal data – GDPR applies before, alongside, and beyond the AI Act

AI Act and other affected legal regimes – relevant in parallel

AI Act
Regulation (EU) 2024/1689 – risk-based, product-safety logic. Up to EUR 35m or 7 % (worldwide annual turnover) for prohibited practices. Phased application 2025-2027.

Civil Liability
Liability: Sec. 280, 311, 823 et seq. BGB; EU Product Liability Directive (EU) 2024/2853 extends strict liability to software/AI; AI Liability Directive withdrawn

Contract Law
Sec. 164 et seq. of the German Civil Code (BGB) on agency: apply only by analogy to autonomous agents. Sec. 166 (attribution of knowledge) unsuitable for probabilistic AI

IP & Trade Secrets
Sec. 2 German Copyright Act: AI-only content generally not protected: human authorship required; § 17 German Trade Secrets Act: Data leakage risk (tool calls)

Anti-Discrimination
General Equal Treatment Act (AGG) prohibits discrimination irrespective of human or AI decisions; burden of proof may shift if AI-driven bias is indicated (Sec. 22 AGG)

IT Security & Cyber
NIS2 (implemented in Germany), Cyber Resilience Act; AI Act (Art. 15): robustness & resilience

The dual compliance stack: GDPR and AI Act apply **cumulatively** – the AI Act does not replace the GDPR (Recital 9 AI Act). For any agent processing personal data, both regimes apply in full.

AI agents under the GDPR

Four critical problems, four concrete pathways

Art. 4(11) Consent

Not “informed”: Agents may read but not understand cookie banners (Sec. 25 TDDDG)

→ Machine-readable signals (Art. 88b GDPR-E); dedicated agent API channel

Art. 5/6 Principles & Lawful basis

Data minimization: hard for agents using dynamic, context-rich data.

→ Privacy by Design (Art. 25); Definition of explicit lawful basis per use case

Art. 12-22 Data subject rights

Art. 15: “Meaningful information about logic”: challenging for black-box models; Art. 17

→ Model cards as standard documentation; Selective deletion of agent memory

Art. 22 Automated decisions

CJEU SCHUFA (C-634/21): score is a "decision" if it materially determines the outcome

→ Map decisions to Art. 22; meaningful human review, not rubber-stamping

» Cross-cutting solution: a DPIA (Art. 35) integrating the AI Act conformity assessment in one document

AI agents under the AI Act

Three classification questions: GPAI, systemic risk, risk-based

QUESTION 1
Is the agent based on a GPAI model?

Test (Art. 3(63)): "significant generality" + competent across "a wide range of distinct tasks"

- If based on an LLM and merely extended for agent function: **GPAI model**
- Fine-tuning alone usually does **not** remove GPAI status – the planning capability requires general capability
- Highly specialized agents may fall outside

Consequence: Art. 53 transparency duties for the model provider

QUESTION 2
GPAI model with systemic risk?

Test (Art. 51 + Annex XIII): high-impact capabilities (>10^{25} FLOP) **or** Commission designation

Annex XIII criteria especially relevant for agents:

- **"Level of autonomy and scalability"**
- **"Tools it has access to"**
- Adaptability to learn new tasks

Outlook: high-performance agents will likely be designated systemic-risk – triggering Art. 55 duties

QUESTION 3
GPAI system | Risk-based class?

Art. 3(66): based on GPAI model, usable for multiple purposes, directly or via integration

Four risk levels (Art. 5-6, 50):

- **Prohibited:** social scoring, manipulation, real-time biometrics. Up to €35m / 7 %
- **High-risk (Annex III):** HR (no. 4), credit (no. 5(b)), insurance pricing (no. 5(c)). Annex III + profiling = **always high-risk** (Art. 6(3)(2)). Up to €15m / 3 %
- **Limited risk (Art. 50):** transparency only
- **Minimal risk:** no specific duties

High-risk duties (Art. 8-15) from August 2, 2026: Risk management (Art. 9), data governance (Art. 10), technical documentation (Art. 11/18), logging (Art. 12), transparency (Art. 13), **human oversight (Art. 14)**, accuracy/robustness/cybersecurity (Art. 15), conformity assessment (Art. 43). **Art. 14(2) paradox:** required oversight scales with autonomy – counteracts the productivity gain agents promise.

» Risk-based approach = intended use, not real capabilities; ignores autonomy & tool access → even "low-risk" agents (e.g. travel-booking agent with system control) can cause severe harm

To-dos for companies

Five integrated building blocks, not two silos

1. **Use-case inventory & risk classification**
   Map use cases; parallel AI Act risk + GDPR DPIA classification; re-classify on tool extension
2. **AI Compliance Officer & governance**
   Dedicated bridge between legal, technology, business; Art. 4 AI literacy duty since Feb. 2, 2025
3. **Human oversight by design**
   HITL/HOTL/HOOTL classification per use case; kill switch as legal requirement
4. **Integrated DPIA + conformity assessment**
   DPIA as platform; AI Act dimensions (Art. 9, 27, 43) integrated; standardized templates
5. **Auditability & vendor governance**
   Structured logging; GPAI duties in vendor contracts

» One integrated process, not two silos. Early legal involvement in use-case selection is the strongest lever

TECH ignite

simmons+simmons

Background:

Agentic is here – and it involves a lot of different areas of law…

When, not if...

62%

Organisations ‘experimenting’ with AI Agents

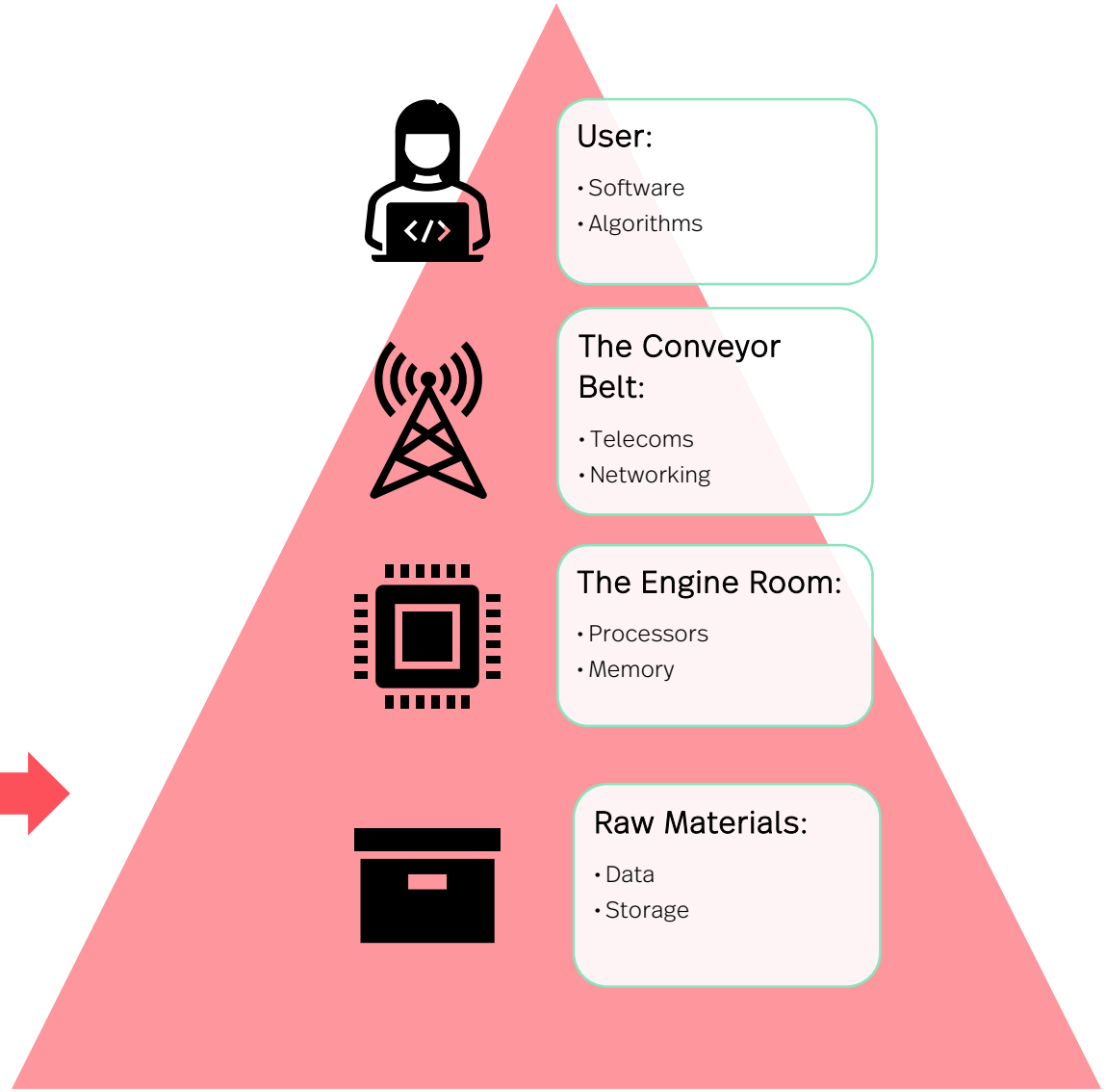
Gartner – December 2025

Agentic AI

Implementing & Running

Agentic AI is not this:

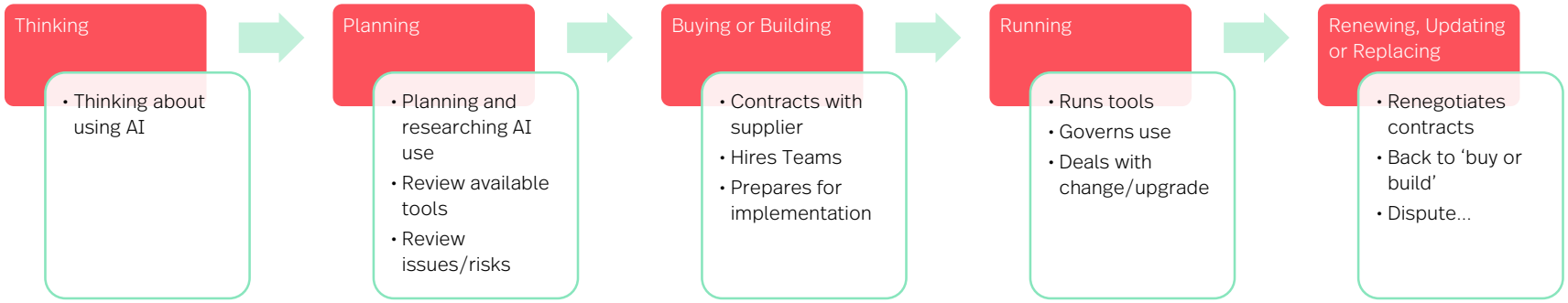
It’s more like this…



AI Law: Transactions

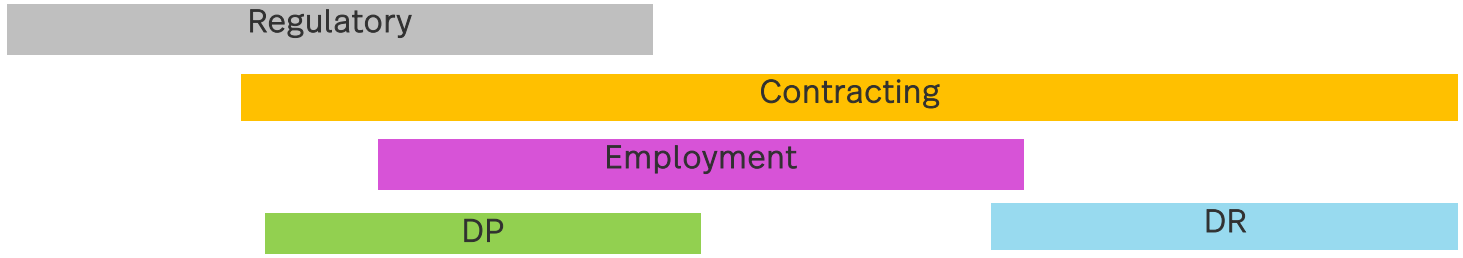
Implementing Agentic AI

Agentic AI



When Legal Input Required

'Typical' Agentic Implementation



TECH ignite

simmons+simmons

Legal Impact:

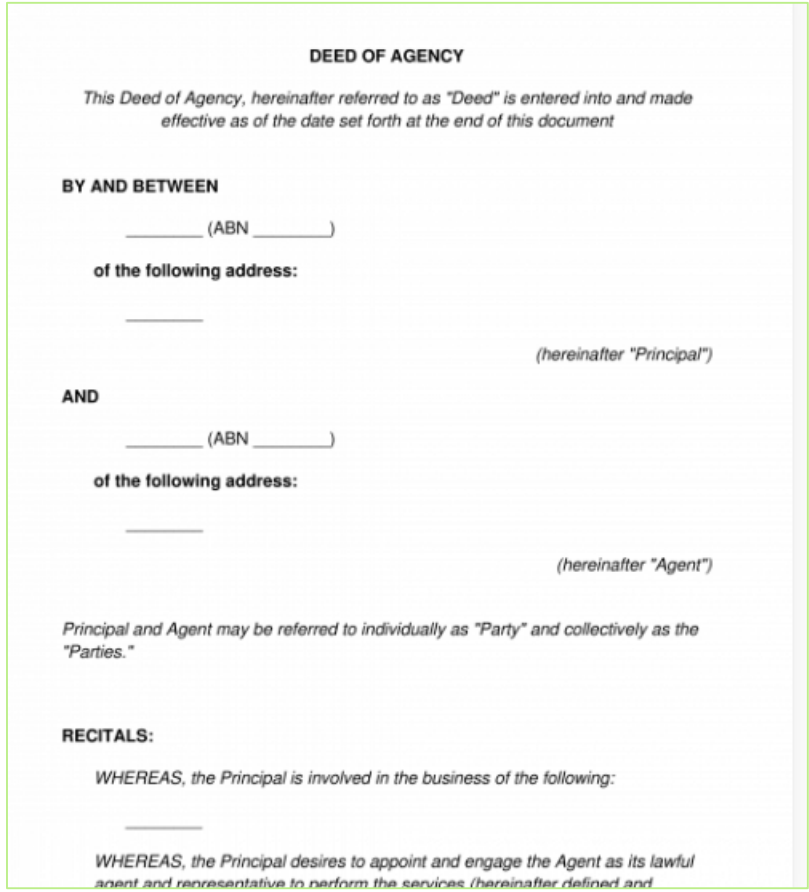
The same, but different...

Same old IT issues?

Agency:

Potential differences:

- Legal personality
- Grant/termination of agency
- EU Commercial Agents Directive (86/653/EEC)



DEED OF AGENCY

This Deed of Agency, hereinafter referred to as "Deed" is entered into and made effective as of the date set forth at the end of this document

BY AND BETWEEN

_____ (ABN _____)

of the following address:

_____

(hereinafter "Principal")

AND

_____ (ABN _____)

of the following address:

_____

(hereinafter "Agent")

Principal and Agent may be referred to individually as "Party" and collectively as the "Parties."

RECITALS:

WHEREAS, the Principal is involved in the business of the following:

_____

WHEREAS, the Principal desires to appoint and engage the Agent as its lawful agent and representative to perform the services (hereinafter defined and

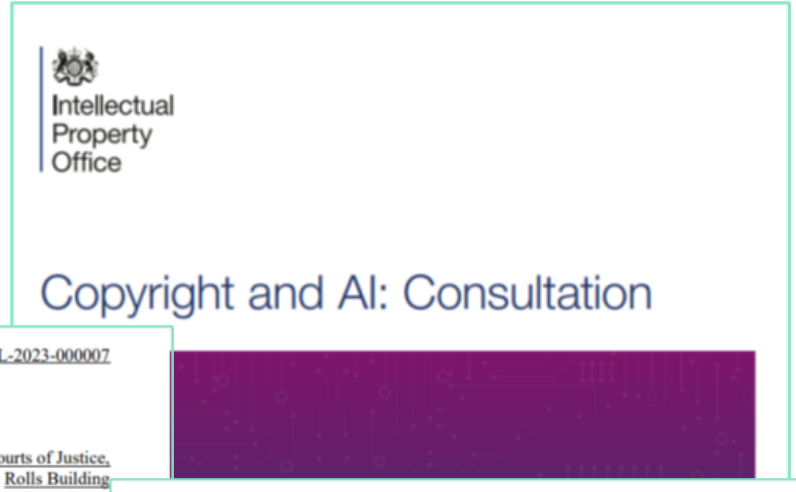
Same old IT contract issues?

Agentic AI

IP:

Potential differences:

- Agentic driven creations
- GenAI and duplicate responses
- IP ownership for GenAI content
- Licensing of training data



Intellectual Property Office

Copyright and AI: Consultation

Case No: IL-2023-000007

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
INTELLECTDUAL PROPERTY (ChD)

Royal Courts of Justice,
Rolls Building
Fetter Lane,
London,
EC4A 1NL

Date: 14/01/2025

Before :

MRS JUSTICE JOANNA SMITH DBE

Between :

(1) GETTY IMAGES (US) INC
(2) GETTY IMAGES INTERNATIONAL UC
(3) GETTY IMAGES (UK) LIMITED
(4) GETTY IMAGES DEVCO UK LIMITED
(5) ISTOCKPHOTO LP
(6) THOMAS M BARWICK INC

Claimants

- and -

STABILITY AI LTD

Defendant

THOMSON REUTERS ENTERPRISE CENTRE GMBH and WEST PUBLISHING CORP.,

Plaintiffs,

v.

No. 1:20-cv-613-SB

ROSS INTELLIGENCE INC.,

Defendant.

Jack B. Blumenfeld, Michael J. Flynn, MORRIS, NICHOLS, ARSHT & TUNNELL LLP, Wilmington, Delaware; Dale M. Cendali, Eric A. Loverro, Joshua L. Simmons, KIRKLAND & ELLIS LLP, New York, New York; Yungmoon Chang, KIRKLAND & ELLIS LLP, Los Angeles, California; Miranda D. Means, KIRKLAND & ELLIS LLP, Boston, Massachusetts.

Counsel for Plaintiffs.

David Ellis Moore, Bindu Ann George Palapura, POTTER ANDERSON & CORROON LLP, Wilmington, Delaware; Jordan Ludwig, Emily T. Kuwahara, CROWELL & MORING LLP, Los Angeles, California; Ryan Henry Seewald, CROWELL & MORING LLP, Denver Colorado; Warrington Parker, Joachim B. Steinberg, Jacob Canter, Christopher J. Banks, Anna Z. Saber, Margaux Poueymirou, CROWELL & MORING LLP, San Francisco, California; Keith J. Harrison, Mark A. Klapow, Lisa Kimmel, Crinesha B. Berry, CROWELL & MORING LLP, Washington, D.C.

Counsel for Defendant.

MEMORANDUM OPINION

February 11, 2025

Same old IT issues?

Limitation:

Potential differences:

- Quantum of €€ – will the error be noticed later?
- Duty to mitigate – what are the reasonable steps to reduce loss?
- Agentic AI and the lack of a ‘fat finger’ rule / law of mistake

Meta’s AI Agent Triggers Security Breach in Hours-Long Incident

Autonomous system posts unauthorized advice, triggers SEV1 incident affecting employee access controls

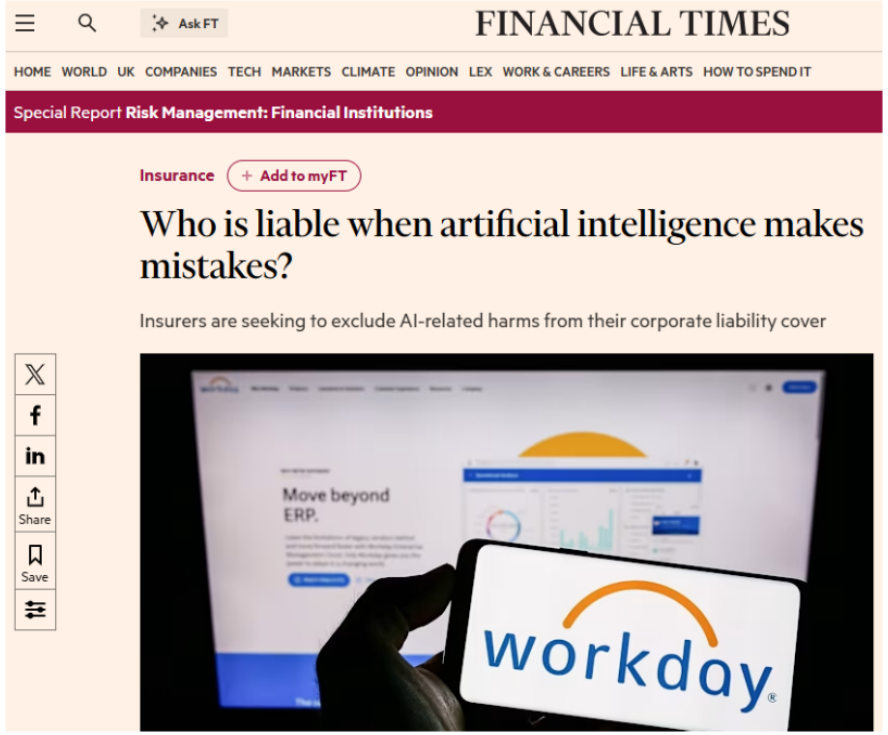
Al Landes Mar 19, 2026 · 2 min read

Same old IT issues?

Exclusion:

Potential differences:

- Causal connection / Adequate Causation
- What can be considered as ‘consequential’ re Agentic AI
- Are ‘reputation’ and ‘third-party contract’ more relevant?



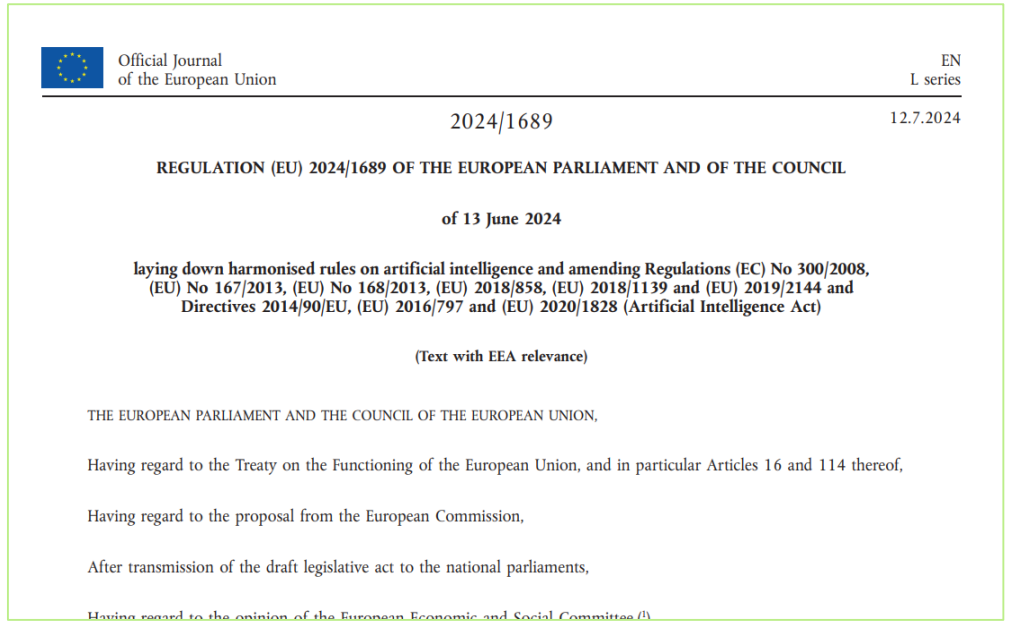
Same old IT issues?

Agentic AI

Compliance with laws:

Potential differences:

- Specific regulatory regime
- Lots of guidelines/enacting legislation still to come



Official Journal of the European Union

EN
L series

2024/1689

12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1)

European Commission

EN

Search

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office

Home > Library > The Commission publishes guidelines on AI system definition to facilitate the first AI Act's rules application

POLICY AND LEGISLATION | Publication 06 February 2025

The Commission publishes guidelines on AI system definition to facilitate the first AI Act's rules application

The guidelines on the AI system definition explain the practical application of the legal concept, as anchored in the AI Act.

By issuing guidelines on the AI system definition, the Commission aims to assist providers and other relevant persons in determining whether a software system constitutes an AI system to facilitate the effective application of the rules.

The guidelines on the AI system definition are not binding. They are designed to evolve over time and will be updated as necessary, in particular in light of practical experiences, new questions and use cases that arise.

GettyImages © Aree Sarak

Same old IT issues?

Change

Change is not new in IT…*but*…

Potential differences:

- Sheer volume/pace e.g. Guidelines re AI, global politics - impact on triggers and timescales

- Supplier change rights linked not just to regulation e.g. case law on IP, market sentiment