Regulatory updates

Recent regulatory developments

Last update: September 2025

Contents

1 Other developments 3
1.1 EU AI Act (AI Act) 3
1.2 EU Data Act (Data Act) 4
2 International Standards on Auditing (ISA) 6
2.1 ISA 240 (revised) 'The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements' 6
2.2 ISA 570 (revised) 'Going Concern' 6

1 Other developments

1.1 EU AI Act (AI Act)

The EU AI Act introduces a risk-based framework for regulating artificial intelligence systems. This legislation sets out the rules for the development, market placement and use of AI in the European Union, aiming to ensure that AI is trustworthy, ethical, and respects fundamental rights.

Status:
- In force since 1 August 2024

Applicability of strict provisions on artificial intelligence

The EU AI Act, which came into force on 1 August 2024, introduces a new regulatory framework for governing artificial intelligence systems. It outlines rules for the development, market placement and use of AI in the European Union. The obligations for providers of general-purpose AI models took effect on 2 August 2025. The majority of the high-risk AI system requirements and full applicability of many enforcement provisions will take effect from **2 August 2026**.

The EU AI Act applies to both providers and users of AI systems operating within the EU, as well as providers and users outside the EU if the output produced by the system is intended to be used within the EU. This extraterritorial scope means that businesses and organisations, including Swiss companies, must comply with the EU AI Act when their AI systems have an impact on EU citizens.

Compliance

The EU AI Act sets out a risk-based approach to AI applications based on the potential risks they pose to fundamental rights, safety and privacy. The AI Act classifies AI systems in four main categories based on the level of risk they pose: unacceptable, high, limited, and minimal risk.

Systems in the '**unacceptable**' risk category that pose significant threats to safety, rights or democracy (such as AI for social scoring by governments) are prohibited. **High-risk** systems used in critical sectors such as healthcare, law enforcement and transport are subject to strict requirements, including risk assessments, data governance and human oversight. These systems will also need to be registered in an EU database of high-risk AI systems.

Limited-risk AI systems, such as those used in chatbot interactions, require transparency obligations, while **minimal-risk** AI systems are largely unregulated.

The AI Act introduces several compliance requirements, such as the obligation to ensure human oversight over AI systems, accurate data documentation and robust risk management processes. Organisations developing or deploying AI will also need to perform conformity assessments for high-risk systems and, in certain cases, self-assessments for lower-risk applications. The European Artificial Intelligence Board will oversee enforcement and provide guidance to both national authorities and companies.

Significant penalties are proposed for non-compliance. Violations of the AI Act, particularly those involving high-risk or prohibited AI systems, could result in fines of up to 7% of global annual turnover or EUR 35 million, whichever is greater, highlighting the serious financial risks for companies that fail to adhere to the regulations.

The EU AI Act aims to balance innovation and public trust by ensuring that AI systems are designed, developed and used in ways that protect the fundamental rights and freedoms of individuals. This regulation will probably have a profound impact on AI innovation throughout Europe, particularly for companies operating in sectors under close regulatory scrutiny or with high levels of consumer interaction. The AI Act also emphasises AI governance, calling for transparency and traceability in AI decision-making, which will require significant technical and organisational efforts from businesses to ensure compliance.

Much like the GDPR, the EU AI Act represents a critical shift in regulatory approach, recognising the transformative power of AI while addressing the risks posed to individuals and society as a whole. The focus on accountability, fairness and transparency resonates in various sectors, and companies will need to adapt their AI governance models accordingly to maintain compliance.

Who will be affected?

Any organisation developing or deploying AI within the European Union will be subject to the AI Act. This includes non-EU organisations that offer AI-based services or products to EU residents, or operate within the EU. For example, a Swiss tech company deploying AI-driven medical diagnostics software in the EU must comply with the AI Act's high-risk classification rules.

What can you do?

To prepare for the EU AI Act, we recommend taking the following steps:

- Analyse AI systems currently in operation or in planning, and identify any high- and limited-risk AI systems within your operations that will be subject to new regulations.
- Ensure that your AI development processes integrate risk management, testing and transparency from the outset.
- Review your documentation and risk assessment protocols to align with the AI Act's standards, particularly for high-risk systems.

Your PwC AI and data protection experts can help assess your current AI systems, guide you through the regulatory landscape and ensure that you comply with the new AI legislation.

1.2 EU Data Act (Data Act)

The EU Data Act aims to create a harmonised framework for data-sharing, access and use between businesses, consumers, and public-sector institutions throughout the European Union. The Data Act focuses on non-personal data, ensuring that data-driven innovation can thrive while maintaining fairness, competition and data sovereignty.

Status:	• In force since 12 September 2025

Applicability of data-sharing rules

The EU Data Act is applicable as of 12 September 2025. The EU Data Act will apply throughout the European Union, establishing rights and obligations for companies and public bodies in relation to the access, sharing and use of non-personal data. The Data Act is particularly relevant for companies developing cloud services, Internet of Things (IoT) products, and other data-heavy technologies.

As with the EU GDPR and the EU AI Act, the EU Data Act will extend beyond the borders of the EU, applying to non-EU companies that operate within the EU or offer products and/or services to EU-based customers. This extraterritorial application ensures that all organisations handling EU-based data adhere to the same rules.

Like the GDPR and the EU AI Act, Swiss companies offering data-driven products or services to the EU market or engaging in data-sharing practices with EU companies will need to comply with the EU Data Act. This ensures that Swiss firms remain competitive and fully compliant when operating in the EU's digital economy.

Compliance

To comply with the EU Data Act, companies will need to:

- Ensure that they have clear processes for sharing non-personal data, especially regarding data portability, access rights and conditions for cloud service switching.
- Develop robust data-sharing agreements that are aligned with the principles stated in the Data Act, ensuring fair access to data by third parties.

Provide transparency regarding data access conditions and ensure that users, whether businesses or consumers, have control over the data generated by their products or services.

The EU Data Act also imposes restrictions on cloud providers regarding data portability, requiring them to facilitate smooth transitions between service providers and prevent data lock-in.

Who will be affected?

The EU Data Act will affect a wide range of industries, particularly those in data-centric sectors such as IoT, cloud computing and AI. Companies that collect, process and store non-personal data will be subject to the new rules, as will public-sector institutions that access data for regulatory or societal needs.

Any company that offers services or products within the EU or handles data generated by EU-based users will need to comply with the Data Act. This requirement extends to non-EU businesses (including Swiss companies) that offer data-driven products or services to the EU market or engage in data-sharing with EU companies.

What can you do?

To prepare for the EU Data Act, we recommend that you take the following steps:

- Review your current data-sharing practices and ensure that they align with the new requirements for transparency and fairness.
- Establish processes for data portability and seamless switching between cloud providers, as mandated by the Data Act.
- Update contracts and service-level agreements with third parties to reflect data access and usage obligations.

Your PwC data protection and compliance team is available to help you assess your current data-sharing strategies, ensuring that your organisation is ready to meet the challenges and opportunities brought on by the EU Data Act.

2 International Standards on Auditing (ISA)

2.1 ISA 240 (revised) 'The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements'

The revised standard is a response to heightened stakeholder expectations for a more robust auditing standard and greater transparency about the auditor's work related to fraud, following various high-profile corporate failures and scandals.

Status:
- Effective for audits of financial statements for periods beginning on or after 15 December 2026

The objectives of the revision were to:
- Clarify auditor responsibilities – Define more clearly what auditors are responsible for regarding fraud in an audit of financial statements.
- Strengthen fraud risk response – Improve consistency and effectiveness in how auditors respond to risks of material misstatement due to fraud, by reinforcing and clarifying requirements in ISA 240.
- Promote professional scepticism – Emphasise the importance of maintaining professional scepticism throughout the audit in fraud-related audit procedures.

Enhance transparency and communication – Improve transparency on fraud-related procedures where appropriate, including strengthening communication with those charged with governance and the reporting requirements in ISA 240 and other relevant ISAs.

2.2 ISA 570 (revised) 'Going Concern'

The revised standard seeks to promote consistent practices and behaviours and therefore includes requirements addressing expanded auditor responsibilities relating to evaluating management's use of the going concern basis of accounting, together with significant new additions to the auditor's report.

Status:
- Effective for audits of financial statements for periods beginning on or after 15 December 2026

The revised standard aims to:
Promote consistency and effectiveness – Encourage consistent audit practices and behaviours as well as effective responses to risks of material misstatement related to going concern.

- Strengthen auditor's evaluation of management's going concern assessment – Reinforce the auditor's assessment of management's evaluation of going concern, with a strong emphasis on exercising professional scepticism throughout the audit.
- Enhance transparency – Improve clarity in terms of the auditor's responsibilities and work related to going concern, including stronger communication and reporting requirements.