

# Regulatory updates

## Recent regulatory developments

Last update: October 2024



# Contents

<b>1</b>	<b>Other developments .....</b>	<b>3</b>
1.1	EU AI Act (AI Act) .....	3
1.2	EU Data Act (Data Act).....	4
<b>2</b>	<b>International Standards on Auditing (ISA) .....</b>	<b>6</b>
2.1	ISA 600 (revised) 'Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors)' .....	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, placement on market 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, placement on market and use of AI in the European Union.

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 in 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 6% of global annual turnover or EUR 30 million, whichever is greater, highlighting the serious financial risks for companies not adhering to the regulation.

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 across 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 across 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: • Entry into force on 12 September 2025

### Applicability of data-sharing rules

The EU Data Act will enter into force on 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 ensure compliance 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 align with the principles set out in the Data Act, ensuring fair access to data by third parties.
- Provide transparency with regard to 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 by the EU Data Act.

## 2 International Standards on Auditing (ISA)

### 2.1 ISA 600 (revised)

#### 'Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors)'

**The standard reinforces and enhances the responsibilities of the group engagement leader with regard to managing and achieving audit quality on the engagement, and the responsibilities of the group auditor in terms of the overall direction and supervision of the group audit, and reviewing the work of component auditors.**

Status: • Effective for audits of financial statements for periods beginning on or after 15 December 2023

The most significant changes made to the standard include:

- The group auditor's responsibility for the group audit along with a change in the definition of the engagement team.
- Greater focus on the 'top-down,' group auditor-led, risk-based approach, involving more extensive and explicit responsibilities for the group auditor in terms of risk assessment and developing responses to the risks assessed.
- Revised requirements and guidance on group audit scoping to facilitate a risk-based approach that provides greater flexibility when developing a group audit plan in order to obtain sufficient appropriate audit evidence (where, what and by whom the audit work will be performed).
- Removal of the concept of 'significant' component and related requirements to identify significant components and perform a 'full-scope' audit of individually financially significant components.
- Removal of 'review of the financial information of the component' as a type of work that may be performed at a component.

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. It does not take into account any objectives, financial situation or needs of any recipient; any recipient should not act upon the information contained in this publication without obtaining independent professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2024 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.