



# Regulatory updates

## Recent regulatory developments

Last update: May 2026



## 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 240 (revised), ‘The Auditor’s Responsibilities Relating to Fraud in an Audit of Financial Statements’.....	6
2.2	ISA 570 (revised), ‘Going Concern’ .....	6
<b>3</b>	<b>New Swiss laws.....</b>	<b>7</b>
3.1	Swiss Investment Screening Act .....	7
3.2	Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners (‘TJPG’) .....	8

# 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, and
- develop robust data-sharing agreements that are aligned with the principles stated in the Data Act, ensuring that third parties have fair access to data.

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)

**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

### 2.1 ISA 240 (revised), ‘The Auditor’s Responsibilities Relating to Fraud in an Audit of Financial Statements’

The objectives of the revision were to:

- clarify auditor responsibilities – define more clearly auditors’ responsibilities 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.

## 3 New Swiss laws

### 3.1 Swiss Investment Screening Act

**The Federal Investment Screening Act aims to prevent takeovers of domestic companies by foreign state-controlled investors if those takeovers would endanger or threaten Switzerland's public order or security (so-called 'Lex China'). The scope of the new law is limited to foreign state investors, while private foreign investors are not affected.**

Status: • The deadline for the optional referendum runs until 17 April 2026. The act can therefore be expected to come into force in 2027.

#### Objective and scope of the Federal Investment Screening Act

The scope of the new legislation applies to takeovers of domestic private and public-law companies by foreign state investors. Domestic companies are defined as companies that are registered in the Swiss commercial register. Foreign state investors are defined as (i) foreign state bodies; (ii) companies with headquarters outside Switzerland that are directly or indirectly controlled by a foreign state body; (iii) companies with assets that are directly or indirectly controlled by a foreign state body; and (iv) natural or legal persons acting on behalf of a foreign state body. The new law does not affect takeovers by private foreign parties, even if the target company operates in a critical business sector.

The new law contains a preventive and risk-based screening of foreign investments. The prerequisite for an investment review by the State Secretariat for Economic Affairs (SECO) is a takeover through which one or more foreign state investors gain direct or indirect control of a domestic company, namely through a merger, the acquisition of a stake or the conclusion of a contract.

A reporting obligation towards the SECO applies only if the target company exceeds certain thresholds and if the target company is active in a critical sector. The legislation distinguishes between (i) security-relevant companies and (ii) critical infrastructures.

- **Security-relevant companies:** In the case of acquisitions of domestic companies in security-critical areas, such as the defence industry, energy and water supply or security-related IT systems, investment control applies if these companies employ at least 50 full-time staff worldwide and have generated sales of at least CHF 10 million in the previous two financial years.
- **Critical infrastructure:** Domestic companies that operate critical infrastructure, such as university hospitals or general hospitals with central care, medical care, transport and logistics infrastructure, food distribution centres, telecommunications networks, or systemically important financial infrastructure (including systemically important banks) are subject to investment control if they have generated an average annual turnover of at least CHF 100 million worldwide in the past two financial years.

The Federal Council reserves the right to subject further categories of domestic companies to SECO's approval requirement if there are sufficient indications at the time of the takeover that the change of ownership could endanger or threaten public order or security.

#### Compliance

To comply with the Federal Investment Screening Act, companies have the following obligations:

- In transactions involving a foreign investor, it must be assessed whether the investor is state-controlled and whether the Swiss company operates in a critical sector and meets the relevant thresholds.
- If the new law applies to the transaction, the screening procedure must be initiated by the foreign investor, who submits an application to the State Secretariat for Economic Affairs (SECO).
- The new law also provides for parties involved in a takeover to have a non-binding assessment conducted to determine whether the takeover is likely to be subject to approval.

In the event of a breach of the law, the Federal Council can impose administrative measures, including divestiture orders, if a takeover is completed without required approval, if the approval was obtained through false information, or conditions attached to an approval are violated. In addition, the resulting company may face administrative penalties of up to 10% of its global annual turnover.

#### **Who will be affected?**

Switzerland is adopting a moderate approach to investment control that is limited to foreign state investors, while private foreign investors remain unaffected. Combined with the thresholds applicable to transactions in critical sectors, only certain deals will require prior approval from the respective authorities.

#### **What can you do?**

To prepare for the Swiss Investment Screening Act, we recommend that you take the following steps:

- Assess whether a planned acquisition falls under the new Swiss Investment Screening Act (scope, state-controlled foreign investor, critical sectors), map ownership/control, and advise on deal structure and timelines to avoid standstill/gun-jumping risks.
- Prepare and manage the filing (authorisation request) to the competent authority, coordinate Q&A, and propose mitigation/commitments if required; align the screening process with merger control and other regulatory clearances.
- Monitor entry into force and forthcoming ordinances.

PwC's legal team is available to help you with any questions related to this topic.

### **3.2 Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners ('TJPG')**

**Switzerland is introducing a central transparency register for the beneficial owners of Swiss and foreign legal entities to comply with international treaties. Under the new law, affected legal entities must identify their beneficial owners and must subsequently report this information to the transparency register.**

Status: • The new law is expected to come into force in the second half of 2026 or early 2027.

## **Objective and scope of the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners**

The Act's objective is to strengthen Switzerland's anti-money-laundering and counter-terrorist financing framework by ensuring that authorities have access to complete, correct and up-to-date information on who ultimately controls legal entities. It establishes a centralised federal beneficial ownership register operated by the Federal Office of Justice, with access for designated authorities and entities and persons falling under the respective obligations. The scope of the new act covers legal entities under Swiss private law, with express exclusions for associations and foundations. It is also applicable to certain foreign legal entities closely connected to Switzerland, including entities with effective management in Switzerland, or with real properties or branches in Switzerland. The TJPG includes certain exemptions from its scope of application. Legal entities with participation rights listed on a stock exchange, as well as subsidiaries held directly or indirectly for more than 75% by such listed companies, are exempt. Pension funds and entities owned by public authorities are also excluded. Additionally, simplified rules apply to legal entities that are partly owned by a listed company. However, the new law will affect a large number of Swiss and foreign companies.

The affected entities have a duty to identify, verify and report their beneficial owners, i.e. natural persons who ultimately hold at least 25% of capital or voting rights, or otherwise exercise control. The affected entities are required to submit to the Transparency Register the name, date of birth, nationality, address, and municipality and country of residence of the beneficial owner, together with information on the nature and extent of the control exercised. The entities must send the notification electronically to the Transparency Register within one month of the entity's being entered in the commercial register or, in the case of a foreign entity, within one month of becoming subject to the TJPG. If there is a change to the information contained in the Transparency Register (e.g. a change of beneficial owner or a change of address of the beneficial owner), the entity must also notify the register within one month of becoming aware of the change. Contrary to its name, the Transparency Register will not be accessible to the public. Access is limited to the authorities specifically designated by law, such as the inspection body, federal and cantonal police authorities, administrative and criminal authorities, and the Money Laundering Reporting Office. Furthermore, financial intermediaries may access data held in the Transparency Register (except for certain deleted data, among other exceptions) online to the extent required for the purpose of performing due diligence.

### **Compliance**

To comply with the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners, companies have the following obligations:

- Duty to identify, verify and report the beneficial owners
- Duty to register their beneficial owners in the new Transparency Register within the given timeline

Since the law will soon enter into force and the transition periods for the required notifications are very short, entities should prepare for the new rules sufficiently early. Otherwise, penalties may be imposed.

### **Who will be affected?**

- Swiss entities such as companies limited by shares, limited partnerships, limited liability companies, cooperatives, investment companies with variable or fixed capital (SICAV/SICAF) and limited partnerships for capital investment schemes
- Trustees domiciled/based in Switzerland or who manage trusts in Switzerland (excluding trustees subject to the AML Act)
- Foreign entities with branches, actual management or real estate in Switzerland

## **What can you do?**

Swiss and foreign entities should identify and verify their beneficial owners against the TJPG's 25% ownership/control standard, prepare the necessary documentation and establish internal processes to report and update this information in the new Federal Transparency Register.

Since the law will soon enter into force and the transition periods for the required notifications are very short, PwC's legal team will be pleased to help you with any questions related to this topic.

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.

© 2025 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.