Digitization, Regulation

Cybersecurity without ***regulatory illusions***

22.01.2026

At a glance

- After years of regulatory consolidation, the EU is increasingly focusing on simplification, harmonization and investment security instead of ever more detailed rules.
- Market-driven measures, international standards and technological expertise contribute more to resilience than increasingly detailed government regulations.
- Switzerland has taken a measured approach in the cyber area so far - it is now crucial not to abandon this approach and not to adopt regulations that the EU itself is already beginning to correct.

The European Union is opening a new chapter in digital policy. After years of regulatory consolidation, there are increasing signs of a course correction. The Digital Omnibus, the announced Digital Networks Act, the revision of the Cyber Security Act and the ongoing digital fitness check represent a clear trend: simplification, harmonization and a stronger focus on investment and implementation instead of ever more detailed rules.

What the EU is now recognizing - and Switzerland should learn from it

A central distorted image still shapes many debates today: cybersecurity only arises when the state forces companies to act. Voluntary measures and market mechanisms would not be enough. In practice, however, the picture is different.

Cybersecurity is not a nice-to-have for companies, but an existential factor. Data loss, production stoppages or reputational damage have direct economic consequences. However, the extent to which companies invest in cyber security and at an early stage differs significantly depending on their size.

SMEs in particular are already under considerable cost and bureaucratic pressure. They often lack the financial leeway to implement complex regulatory requirements in cyber security at an early stage. Additional detailed regulation is of little help here. Awareness-raising, guidance and easily accessible information that enables risks to be managed proportionately and gradually are more effective. In addition, international standards and certifications such as ISO 27001 or NIST frameworks often go far beyond the minimum legal requirements.

Modern cloud and security providers also operate global security operation centers and invest billions in attack detection, redundancy and automation. This level of security is the result of proximity to technology and rapid adaptability - not annual administrative requirements.

This does not mean that the state has no role to play. It is needed where market mechanisms reach their limits: with minimum standards for critical infrastructures, clear responsibilities and transparency. What it cannot do, however, is provide operational cyber security in everyday life. Threats develop faster than regulation.

This is precisely where the European change of course comes in. The Cyber Resilience Act illustrates the EU's learning curve particularly clearly. As a complex and bureaucratic intervention in the product life cycle, it was sharply criticized by the business community. The fact that the EU is now taking these objections on board is less a success of the instrument than an admission that overloaded regulation is becoming a disadvantage for business locations.

A veritable paradigm shift

It's not about deregulation, but about location policy. Security comes from reliability, not from ever new obligations. Investments in cyber security are made where companies know where they stand.

The EU's rethinking of regulation in the digital space is a warning signal - not because Switzerland is going it alone today, but as a reminder not to abandon the current course. In the cyber area, Switzerland has done well not to rush ahead and to implement European requirements with a sense of proportion. It is now crucial not to take on the regulatory legacy that the EU itself has recognized as too complex and has begun to correct.

Angela Anthamatten

Deputy Head of Department Competition & Regulatory Affairs

David Stauffacher

Project Manager infrastructure and digital