AI Compliance in Companies (Part III) – Scope of the GDPR and AI Act?

Navigating the EU's AI Regulatory Landscape

The European Union's regulatory environment for artificial intelligence is complex, primarily shaped by two key frameworks: the General Data Protection Regulation (GDPR) and the new Artificial Intelligence Regulation (AI Act).

While the GDPR has long been the established standard for personal data handling, the AI Act is the first comprehensive regulation specifically designed for AI systems.

Both regulations share overarching goals, such as safeguarding fundamental rights and fostering trust in new technologies.

A crucial question arises when AI systems process personal data (often their "fuel"): whether compliance with one regulation is sufficient, or if new, overlapping obligations will emerge.

Understanding the GDPR's Scope and Focus

The GDPR's primary focus is on the processing of personal data, defined as any information related to an identified or identifiable natural person.

"Processing" encompasses nearly any handling of personal data, including reading, storing, transferring, and deleting.

The GDPR is designed to be technology-neutral, applying its provisions regardless of the specific technology used, provided personal data is involved.

The GDPR is designed to be technology-neutral, applying its provisions regardless of the specific technology used, provided personal data is involved.

Understanding the AI Act's Scope and Focus

In contrast to the GDPR, the AI Act primarily regulates AI systems and AI models themselves.

An AI system is defined as a machine-based system operating with varying autonomy, capable of adaptiveness, and generating outputs like predictions or decisions from input.

While not directly defined, AI models are central components of an AI system, essentially representing the neural network and core of the system.

The AI Act functions as a product safety law, establishing uniform rules for placing AI systems and models on the market, putting them into service, and their use within the EU.

Regulatory Approaches and Risk Management

AI Act Approach

The AI Act focuses on classifying AI systems and models into specific risk categories, each subject to distinct legal frameworks.

It defines "risk" as the combination of the probability of damage occurring and the severity of that damage.

GDPR Approach

The GDPR, for its part, requires data controllers to implement technical and organizational measures to address risks to data subjects.

For the use of new technologies, including AI, a well-documented Data Protection Impact Assessment (DPIA) must be considered under the GDPR.

The Interplay Between GDPR and AI Act

The GDPR and AI Act are closely linked in areas where AI systems process personal data, as personal data often serves as the "fuel" for AI.

Both laws share the fundamental goal of minimizing risk, though they achieve this through different approaches.

The AI Act complements the GDPR by specifically addressing the unique risks posed by AI technologies themselves.

Therefore, compliance with one regulation is generally not sufficient; companies face new, potentially overlapping obligations.

Contacts

Anton Schröder

German Attorney at Law,
Associate at FIN LAW

FIN LAW

Auffenberg und Uhink
Partnerschaftsgesellschaft
von Rechtsanwälten mbB

Senckenberganlage 19
60325 Frankfurt am Main

E. info@fin-law.de

I. https://fin-law.de

T. +49 69 87 000 1320