



COMPETITION

AI and the Data Privacy Elephant in the Room

17 July 2025 2 min read

"The real problem is not whether machines think, but whether men do." – B.F. Skinner

by Ahmore Burger-Smidt, Director and Head of Regulatory

Insights from the *2025 Report: AI Risk & Readiness in the Enterprise*^[1] Underlines the exponential threat that is not being addressed by AI progress. Data Privacy, a pressing issue that demands immediate attention!

From data leaks to regulatory "*blind spots to shadow AI running amok*", the report highlights the fact that there are risks that cannot be ignored while organisations move towards the adoption of AI.

But what are these risks? More importantly, the question should be asked how to identify these risks.

Understanding and visibility into how AI models interact with personal data and sensitive personal data are crucial in identifying risks from a data privacy perspective. Without such insight, organisations will remain blind to data privacy risks within their environment, significantly increasing the risk associated with exposure to unauthorised use, access or further processing of personal information and data breaches.

The more data an AI model relies on, the higher the risk of exposing personal data and sensitive personal information. Shadow AI, meaning unauthorised or unmonitored AI use and tools, further compounds the above risk by operating outside of the organisation's security visibility.

One of the core outcomes of the Report is the alarming statistic that 69.5% of organisations surveyed rank AI-powered data leaks as their biggest security concern.

As such, data leaks remain the most feared threat, informed by AI's interaction with unstructured data and the rise of unauthorised models. But what to do?

Mitigating against data privacy breaches requires an understanding of what specific data is used for the particular AI model. Also, what the internal and external rules are in relation to the use of personal data and what the lawful basis is for doing so.

Organisations must conduct data privacy impact assessments to gain the necessary insight into privacy risk when considering AI. These assessments are a powerful tool in limiting the risk of exposure and detecting rogue model activity that could result in a data breach. Therefore, they are a crucial part of ensuring compliance with privacy legislation and protecting data subject rights.

The message: Understand what data the AI model relies on.

Read more about our [Regulatory](#) practice area.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)