Interview Ecosystem Supporter

AD FONTES

GOLD SPONSOR

We see in our practice that EU-providers can in fact carve out a strong market position by offering tangible compliance evidence with concrete and GDPR based explanations of data flows and relevant certifications. Choosing a trusted cybersecurity provider strengthens customers' trust in the company and is a building block for an approach that integrates data privacy compliance and cybersecurity in the long term.

You operate at the interface between cybersecurity and law. How are both interrelated?

Cybersecurity focuses on preventing unauthorized access and protecting systems, while data privacy ensures personal data is handled lawfully and ethically. Even though the scope is different - cybersecurity protects all data and systems, while privacy focuses on individuals' rights over personal data - both are strongly interconnected: Privacy regulations, like GDPR, or the various new EU regulations, drive cybersecurity priorities by defining protection requirements. Strong cybersecurity measures are vital for asset protection but also for achieving data privacy, as breaches compromise personal information. Due to this interconnection, it is so important for us to create a holistic approach allowing our clients to address both topics at the same time.

How can companies effectively manage both the risks posed by cyber threats and those arising from non-compliance with European and national legal rules?

In both domains - cyber threat landscape and EU/national regulation - complexity is growing at a fast pace. The EU has recently adopted several key measures, as the NIS2 directive or the Cyber Resilience Act, which aim to constitute a comprehensive approach to bolstering cybersecurity. Those regulations impose significantly stricter cybersecurity obligations on companies and increase C-level liabilities. Also the AI Act requires AI systems to comply with cybersecurity standards. In fact, cybersecurity is becoming law. We think this is a positive development in today's digital landscape, where cyber threats are increasingly sophisticated and pervasive. Our value is to help our clients operate in good balance between more or less flexible regulatory mechanisms and innovation and security needs.

What first steps would you recommend for a EU based medium-sized company that doesn't yet have a comprehensive technical and regulatory cybersecurity strategy?

The first crucial step is for the management to acknowledge cybersecurity as a strategic priority. This requires understanding the potential financial, operational, and reputational risks posed by cyber threats and regulatory non-compliance. For this purpose we conduct for our clients leadership briefings or workshops, emphasizing the importance of a comprehensive strategy. Operational kick-off is typically a risk assessment identifying assets to protect, risks and gaps. Such assessment is for example the CyberRiskCheck developed by the German BSI, ideally in combination with a Privacy Check. This is a standardized risk check, specifically developed for middle-sized companies. After an interview session, the company receives a report containing the score and concrete recommendations, structured according to urgency. The CyberRiskoCheck enables a company to determine its own IT security level, highly relevant for cybersecurity insurability or funding rounds. It is a method recommended by German BSI to approach the NIS2 cybersecurity requirements.

Many U.S.-based cybersecurity providers seem often less transparent about their data processing while European providers tend to prioritize privacy. What criteria should companies use when choosing a cybersecurity service provider?

Outsourcing cybersecurity to a provider is a strategic choice. It gives access to advanced tools and technologies and allows the company to focus on its core business. The choice of providers should follow a structured process. Security capabilities, adaptability, scalability and pricing are essential procurement criteria but shall be completed by clear compliance requirements as companies are responsible for GDPR compliant processing of their providers. Compliance criteria are in particular minimization principles, data privacy policies, data sharing with third parties, auditability and transparency on encryption standards. We see in our practice that EU-providers can in fact carve out a strong market position by offering tangible compliance evidence with concrete and GDPR based explanations of data flows and relevant certifications. Choosing a trusted cybersecurity provider strengthens customers' trust in the company and is a building block for an approach that integrates data privacy compliance and cybersecurity in the long term.

AD FONTES
Rechtsanwälte | Avocats à la Cour

Ad Fontes is a law firm based in Berlin and Paris, specialized in international business, labour, and corporate law. Founding partner Grit Karg is a renowned expert in data privacy, compliance, and digital regulation. Ad Fontes stands out by offering an integrated approach to cybersecurity with Sven Zehl, a recognized expert with extensive knowledge in cybersecurity and compliance. Core services include the CyberRiskCheck and PrivacyCheck.

adfontes.law

Grit KARG
Partner
Ad Fontes

Sven ZEHL
Cybersecurity Expert
Ad Fontes