Five Tips for Addressing Information Security in Service Contracts

Data security must extend beyond the scope of a company's own office or network and to any of the company's service providers that have access to its data, warns **Armand J. (A.J.) Zottola** in Venable LLP's **Digital Rights Review**.

"A company can be held responsible for a data breach involving its own data, regardless of whether the company is directly responsible for managing its own data," Zottola writes. "The risks associated with sharing data with a service provider are best managed through the utilization of contract provisions governing information security."

In his article, he offers guidelines to consider throughout the process of drafting information security provisions to govern the management, handling, and control of a company's data.

Headings for those guidelines include: research applicable legal requirements, set and meet minimum security standards through the establishment of an information security program, ensure the service provider isn't misusing data, determine security breach response procedures, and create audit requirements.

Read the article.

Join Our LinkedIn Group