The Impact of Remote Workforce on Contractual Obligations

03.27.2020

As a significant number of employees are working remotely due to COVID-19, maintaining adequate cybersecurity measures has been a priority for many businesses. Such concerns are certainly justified, and every effort should be made to maintain the integrity and security of a company's network and systems from a technical standpoint.

However, it is also important to confirm that such remote operations do not violate the terms of any contracts, licenses or other agreements that a company has entered into with respect to data (personal or otherwise) it collects, uses or stores. This is particularly relevant for agreements that have been entered into in the last two to three years, as there has been a significant increase in contractual obligations being imposed on companies with respect to data.

For example, some agreements specifically provide that data must reside on a company server and/or in a specific location. Given the current environment, there may be a business or technical reason to want to store that data somewhere else.

Similarly, contracts – such as Data Processing Addendums – may provide that data will only be shared with certain designated third parties. Again, business or technical imperatives may require that the data be accessed or shared more broadly; for example, with companies that provide remote office or videoconferencing capabilities.

In addition, for both operational and redundancy purposes, organizations may need to expand the scope of employees that have access to third party data. If that decision is made, it is important to make sure that such employees have been properly trained as required under applicable agreements.

Being mindful of a company's contractual obligations with respect to data includes cybersecurity. For example, even if a data breach typically does not require notification under state data breach laws, it may trigger a contractual obligation or cause a breach of contract in this current environment.

A company might have several alternatives if it finds that it has contractual obligations with respect to the data that are difficult to comply with due to supporting a remote workforce. In some cases, it may

simply need to notify the third party of the new operating environment; in others, it may need the third party's consent. If obtaining such consent is not possible or is likely to result in an unwanted renegotiation of the agreement, counsel may need to work with others in the company to devise operational or technical workarounds.

If you have any questions about these issues, please contact Kevin Pomfret.

Please note: This alert contains general, condensed summaries of actual legal matters, statutes and opinions for information purposes. It is not meant to be and should not be construed as legal advice. Readers with particular needs on specific issues should retain the services of competent counsel.

Please click here for additional legal updates from Williams Mullen regarding COVID-19.

Related People

- Kevin D. Pomfret – 703.760.5204 – kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity
- Corporate