Legal Considerations for Rapid Implementation of Remote Work Technologies

Over the past few days, companies in every sector and industry worldwide have begun to shift their workforce to working remotely in response to the rapid spread of the Coronavirus (COVID-19). In addition to changing their work cultures and employment practices seemingly overnight, many companies also had to quickly make important decisions with respect to the deployment and use of technologies that will enable work to continue as smoothly as possible. For example, many companies are turning to video and chat communication providers such as Zoom and Slack to enable better remote communications between internal teams and with customers.

In these uncertain times, there is no margin for error and no time to waste as business continues to slow down. Thus, these decisions are crucial for every organization. However, when deciding on the deployment of certain technologies, it is still important to evaluate and conduct due diligence on the technology and vendor in question and determine whether the use of the technology is appropriate for the type of work that needs to be done and the specific industry in which it will be used.

The following are some key legal issues every company should consider when evaluating the rapid deployment of technology:

Terms of Service:

Despite the need to move quickly to begin using a service which might be crucial for a company to continue operating smoothly, it is still extremely important to review the vendor's terms of service to ensure that it does not contain onerous terms and conditions. The company should ensure that it has a way to cancel the agreement if needed and to avoid automatic renewal of the agreement if it does not wish to renew. Additionally, the company needs to evaluate and understand the limitations of liability, indemnification obligation, and warranties provided by the vendor as well as important provisions regarding intellectual property protection and confidentiality. If the terms offered by the vendor are not acceptable and the vendor is unwilling to negotiate changes, the company will need to decide, after considering the legal and business implications, whether to proceed with the vendor's technology.

Data Use, Privacy and Security:

Before proceeding with any vendor and technology, the company needs to understand how its data and its customer's data will be processed and used by the vendor. If the vendor determines that the vendor's data processing and use of data contradicts certain obligations and commitments made by the company to its customers, then it may be risky to proceed with the particular vendor and its technology, no matter how useful it is. Additionally, the company may need to analyze whether the way data is used and

processed by the vendor complies with specific data privacy laws (such as the GDPR in Europe and the CCPA in California, for example).

Industry-Specific Compliance:

Depending on the company's field of operations, its adoption of a new technology may be subject to additional laws and regulations which will require further analysis and review.

For example, a digital health or health IT company that handles patients' protected health information (PHI) will need to ensure that the implementation of a new technology will be done in compliance with the HIPAA privacy and security rules. Prior to signing a contract with a specific vendor, the company will need to ensure that the vendor has taken the steps necessary to comply with HIPAA. Additionally, the company will need to enter into a business associate agreement (BAA) with the vendor and ensure that the way patients' PHI is used and disclosed by the vendor are done in accordance with HIPAA and the BAA entered into between the parties.

Although moving fast is a must in these uncertain times, skipping the necessary due diligence steps prior to engaging a technology vendor could present avoidable additional and unnecessary legal risks.

Guy Milhalter
Partner
GMilhalter@PearlCohen.com
646-878-0814