Monica Zent: Legal Considerations for Remote Companies

It's Crucial for Companies to Re-assess Their Legal Checklist


Monica Zent

SUNNYVALE, CALIFORNIA, UNITED STATES, December 20, 2022 /EINPresswire.com/ -- As a leading attorney and innovator in the legal industry, Monica Zent saw an opportunity in 2002 to re-engineer the law firm concept to create ZentLaw by creating one of the earliest Alternative Legal Services Provider (ALSP) models. By merging the efficiencies and flexibility of outsourcing and remote work with the best attributes of a law firm, ZentLaw offers a better way to practice for attorneys and corporate legal departments, and a winning proposition for its clients. During that time Monica Zent learned many lessons about the remote work environment long before the pandemic.

According to Monica Zent, "There are some key legal considerations that any company needs to consider if it operates in a hybrid or remote work environment." She added, "A proactive approach to security and privacy is paramount to protecting your company, employees, and clients."

> A proactive approach to security and privacy is paramount to protecting your company, employees, and clients."
>
> *Monica Zent*

Many companies have chosen to remain virtual at least in some capacity in the wake of the pandemic, some choosing a "hybrid" work environment and some sticking with fully remote operations and a remote workforce. As a result, companies have tapped into a wide array of remote work and collaboration tools, but there are some important legal ramifications that need to be considered. Remote companies

must re-calibrate their legal checklist and make sure they're taking the necessary precautions to protect themselves, their employees, their clients, and their data.

From Zent's experience, these are a few of the most important legal considerations for remote and hybrid companies:

Evaluate the Strength of Your Authentication

Authentication is an important line of defense in ensuring control of who accesses your business network, communications, and data. If you haven't implemented two-factor authentication, you should consider doing so.

Two-factor authentication (2FA) is a security process in which a user provides two different authentication factors to verify their identity. This helps to ensure that the user is whom they claim to be and helps prevent unauthorized access to the user's account.

There are several different types of authentication factors that can be used for 2FA, including:

Something the user knows: This could be a password, a PIN, or a security question.

Something the user has: This could be a physical token, such as a key fob or a one-time password (OTP) generator, or a digital token, such as a code sent to a phone or email.

Something the user is: This could be a biometric factor, such as a fingerprint or a facial recognition scan.

Implementing 2FA can help protect your business against unauthorized access to your network, communications, and data. It is a good idea to require 2FA for all user accounts and to use multiple authentication factors whenever possible. You should also regularly update and review your 2FA policies and procedures to ensure they are effective and secure.

Consider Network Security

It's important for companies to consider their business privacy and security needs when managing network security for a remote workforce. One option for ensuring secure access to company resources is to use virtual private networks (VPNs). VPNs create a secure, encrypted connection between a device and a network, allowing employees to access company resources as if they were on the company's internal network. This can help protect against unauthorized access and data breaches.

Another option for securing remote access is to use secure networks, such as those provided by a managed service provider or a cloud-based solution. These networks can provide an additional layer of security by separating company data and resources from the public internet.

It's also important to consider the security of employees' home Wi-Fi networks. If you're not comfortable with employees accessing your network on their own at-home Wi-Fi connections, you may want to provide them with secure, company-provided internet access or require them to use a VPN when accessing company resources.

Regardless of the approach you choose, it's important to regularly review and update your security measures to ensure that they meet the evolving needs of your business and remote workforce. It's also a good idea to provide employee training and resources to help them understand the importance of cybersecurity and how to protect company data and resources.

Confidential Information

It's important for companies to establish guidelines for where employees can and cannot communicate confidential information. In general, it's best to confine these kinds of conversations to traditional channels, such as phone or encrypted email, to ensure that they are secure and private.

If you do need to discuss business matters over chat, it's important to use secure platforms and establish guidelines for what types of conversations and content can or cannot be shared. As a general precaution, it's a good idea to limit chat discussions to nonspecific information and to avoid sharing any private, confidential information or links to documents.

It's also important to ensure that employees understand the importance of protecting confidential information and to provide them with the tools and resources they need to do so. This might include training on secure communication practices and the use of encrypted communication tools.

In addition to establishing guidelines for the use of chat platforms, it's also a good idea to have policies in place for the handling of confidential information in general. This might include guidelines for storing and accessing confidential documents, as well as procedures for handling sensitive data and responding to potential data breaches. By taking these precautions, you can help protect your company's confidential information and maintain the trust of your clients and partners.

Data Storage

It's important for companies to store their data in a secure location to protect it from unauthorized access and data breaches. This is especially important for data that includes sensitive client information.

There are several options for storing data securely, including network-attached storage (NAS) and cloud storage.

NAS is a type of storage system that is attached to a network, allowing multiple users to access the data it stores. NAS systems typically offer a range of security features, including user authentication, data encryption, and access controls, to help protect the data stored on them.

Cloud storage is another option for storing data securely. Cloud storage providers typically offer a range of security measures, such as data encryption, access controls, and monitoring, to help protect the data stored in their systems. Cloud storage can be especially useful for remote workers, as it allows them to access data from any location with an internet connection.

When selecting a storage solution, it's important to consider the security measures in place and the level of protection they provide for your data. You should also consider the accessibility and reliability of the solution, as well as any potential cost implications. By carefully evaluating your options and selecting a secure storage solution, you can help protect your company's data and maintain the trust of your clients and partners.

Automate

Automating business processes can help improve efficiency, reduce the risk of errors, and enable employees to work remotely. By automating established processes, you can eliminate the need for manual input and reduce the reliance on employees being physically present in the office.

There are many different types of business processes that can be automated, such as systems that incorporate automated approval capabilities to allow executives to approve contracts or other matters remotely. Other examples might include automated invoicing, payment processing, and customer relationship management (CRM) systems.

To automate business processes, you'll need to identify which processes can be automated and determine the best way to do so. This might involve using software tools or integrating with existing systems. It's important to carefully assess the potential benefits and any potential costs or challenges associated with automation before implementing any changes.

Automating business processes can be a complex undertaking, but it can bring significant benefits to your organization. By carefully planning and executing your automation efforts, you can help improve efficiency, reduce the risk of errors, and enable your employees to work more effectively, even when they're not in the office.

The Bottom Line

It's important for companies to take steps to protect their businesses, employees, and clients as they continue with remote operations, whether partially or fully. There are a variety of measures and precautions that companies can take to help ensure the security and privacy of their operations. Some simple steps that can go a long way in protecting businesses and employees

include:

- Implementing two-factor authentication (2FA) to protect online accounts
- Establishing guidelines for the use of chat platforms and secure communication practices
- Storing data in a secure location, such as network-attached storage (NAS) or cloud storage
- Automating business processes to improve efficiency and reduce the risk of errors

As companies continue to operate remotely, they may discover additional insights about what works best for their workforce and business model. It's important to regularly review and update your security measures and practices to ensure that they are effective and meet the evolving needs of your business. By taking a proactive approach to security and privacy, you can help protect your company, employees, and clients.

About Monica Zent

Monica Zent, founder of ZentLaw, ZentLaw Labs, and LawDesk360, is a respected attorney, businesswoman, entrepreneur, investor, trusted legal advisor to leading global brands, and a legal industry pioneer. Monica Zent dedicates much of her time and talent to various charitable causes. She is a diversity and inclusion advocate, inspiring all people to pursue their dreams.

When Monica Zent saw a legal market that was ripe for improvement and in need of healthy competition, she envisioned a new business model. In 2002, Zent re-engineered the law firm as we know it to create ZentLaw.

By merging the efficiencies and flexibility of outsourcing with the best attributes of a law firm, ZentLaw offers attorneys a better way to practice along with a winning proposition for clients. By providing businesses with expert counsel ready to provide expert support, counsel, and oversight on even the most complex transactional issues and tasks across practice areas, ZentLaw adds value for its clients every day.

ZentLaw is proud to be a WBENC-certified and women-owned business.

More information about Monica Zent: https://officialmonicazent.com/.
Monica Zent on LinkedIn: https://www.linkedin.com/in/monicazent/
Monica Zent on Twitter: https://twitter.com/monicazent
Monica Zent on Facebook: https://www.facebook.com/monica.zent.1/
Information about ZentLaw and Monica Zent: https://zentlawgroup.com/monica-zent/

J Kraft
ONE400
email us here
Visit us on social media: