CARLTON FIELDS

# Workforce Sheltering in Place? Keeping Privacy in Place During COVID-19

March 23, 2020


Companies across the United States and around the globe are having to take the unprecedented step of immediately having a majority, if not all, of their workforce work from home during the COVID-19 pandemic. Emergency orders and shelter-in-place declarations are necessitating a flexibility that has never been seen before; but with this new at-home workforce, it is important to keep in mind not only privacy issues that were imperative before the pandemic but also new privacy issues that have emerged as a result of the crisis.

1. **Work Has Not Suspended and Neither Have Privacy Laws**

Doors are still open for business, even if virtually, and so are regulators. The California Consumer Privacy Act (CCPA) is still in effect, and nothing has been indicated from either the Legislature or the attorney general's office that anything has changed. Other state legislatures are looking to emulate the CCPA in their jurisdictions.

One such jurisdiction is New York, which is not only contemplating privacy legislation but also enacted stringent security requirements. New York's SHIELD Act went into effect on March 21 and calls for companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information." With the indefinite timeline of restrictions that are dictating the new work-from-home environment, employing reasonable security safeguards to protect the personal information of customers and employees is paramount.

As more businesses shift their core business model online, this may trigger regulatory obligations related to the personal data of your customers. Many businesses taking online orders, particularly restaurants, may be collecting personal data in ways they never have before.

The adoption of new cloud services to facilitate information sharing across departments with a distributed workforce may also change the nature of your regulatory responsibilities relating to customer data.

*Tip: Check with legal counsel on any upcoming regulatory implementations. Depending on your industry, check to see if any regulatory requirements have been temporarily suspended due to the national emergency.*

2. **Gut Check: Does Your Company *Really* Have Appropriate Privacy Practices and Procedures in Place?**

In the normal course of day-to-day business operations, privacy compliance often gets swept aside, even when companies appreciate the necessity of compliance and the risk of not doing so. Yet privacy compliance is a business reality that must be confronted as companies are now being forced to switch their workforces to remote work.

As the timeline of directives and orders of the new work-from-home reality are not yet fully defined, creating policies and procedures in the next week or two is essential to help manage what could be weeks or months of managing personal information in a distributed environment.

*Tip: Review your privacy practices and procedures. If you have not developed practices and procedures, consult legal counsel.*

*Tip: If you think your privacy compliance program is up to speed, think about contingency planning. What happens if critical employees to your privacy and security program are no longer able to perform their responsibilities?*

3. **Prepare Your Team With a Reminder of the Company's Privacy Practices**

While some companies provide yearly trainings on company privacy practices and regulations, many employees may not remember the ins and outs of these policies. By creating written, audio, video, and other materials that are easily digestible, you can remind employees that even though they are off-site, privacy should still be top of mind.

*Tip: Send an email to your team reminding them of the company's privacy practices. Highlight some quick tips that employees can act on right away.*

4. **From Conference Room to Videoconference: Know Your Software**

With employees off-site, companies have turned to videoconferencing software and video chat tools to conduct business. These tools are taking the place of conference rooms but may not necessarily have the same privacy protections as a confined conference room where you can see the participants and close the door.

*Tip: Make sure you are vetting the tools that you decide to use to connect remotely. Some considerations include:*

- *What are the privacy practices of the videoconferencing software provider?*
- *Do they have granular administrator controls that ensure privacy?*
- *Can you control employee access to outside parties?*
- *Can you create individualized login accounts for your team so that you can authenticate who is participating?*
- *Are employees being instructed to clear their desktops when screen sharing to avoid sharing information that should not be public or shared with other employees?*

**Conclusion**

In this difficult time, it is important to not lose sight of privacy compliance obligations, many of which have become more challenging with COVID-19, while other, new privacy issues have emerged. The following checklist may help your organization discharge those obligations:

Checklist

- Do you have internal privacy policies and procedures in place?
- Have you educated your employees on these policies and procedures?
- Have vendors been vetted for their privacy and security practices?
- Have you worked to comply with the CCPA and other privacy regimes?

Carlton Fields' Cybersecurity and Privacy Practice is immediately ready to consult and help your company get these resources up to speed during COVID-19.

## Related Practices

Cybersecurity and Privacy
Labor & Employment