Procopio®

CYBERSECURITY AND PRIVACY CONSIDERATIONS DURING COVID-19 PANDEMIC

A brief overview of key considerations for businesses during the COVID-19 pandemic

Elaine F. Harwell, CIPP/US, CIPM
elaine.harwell@procopio.com
619.906.5780

Agenda

- Key cybersecurity considerations during COVID-19 pandemic
  - Remote workers
  - Hidden risks
- COVID-19 Impact on Global Privacy Laws
- COVID-19 Impact on Enforcement of CCPA?

Cybersecurity Concerns – Remote workers

- Identify gaps for your newly remote workforce
  - Update (or create) guidelines for working from home; for example, BYOD; information security policies; and data destruction policies)
  - Ensure access controls are in place
  - Review incident response plans and business continuity plans
- Encourage employees to consider basic privacy and security best practices
  - Change default passwords on home routers
  - Remind employees that phishing attacks are rising rapidly; consider refresher training on how to detect phishing

Cybersecurity Concerns – Remote workers

- Implementing new technologies? Be aware of privacy laws surrounding collection of personal information
  - Biometric laws in Illinois, Texas and Washington
  - Considerations surrounding geolocation data
- Maintain the organization's cybersecurity hygiene
  - Install relevant security patches to address known vulnerabilities
  - Implement 2FA or multi-factor authentication

Cybersecurity Concerns – Hidden risks

- Consider how to maintain confidences in home working environment
  - Conference Apps (Zoom)
  - Connected devices (Alexa, Nest)
  - Paper shredders
- Watch out for proliferation of sensitive or confidential data saved in unauthorized places: personal accounts or on personal devices
  - Puts data out of the organization's control
  - Risks violating laws and regulations
  - Remind employees of what data the organization considers to be sensitive or confidential

Global Privacy Laws – Some relaxed, but still in effect

- Europe's General Data Protection Regulation (GDPR)
  - Business with physical offices in Europe need to check with local data protection authorities about collection of data
  - Different approaches taken in different member states
- State Data Breach Laws
  - Obligations to identify, detect and report breaches remain
  - With workforce remote, ensure someone is still monitoring the network
- HIPAA
  - For covered entities, the US Department of Health and Human Services released a bulletin in February addressing HIPAA Privacy in the context of the COVID-19 and issued a notice in March regarding the exercise of its enforcement discretion in the area of telehealth

Global Privacy Laws – Some relaxed, but still in effect

- California Consumer Privacy Act (CCPA)
  - Still in effect as of January 1, 2020
  - Response to any consumer requests still subject to the law
    - In general, acknowledgment within 10 business days of receipt, response within 45 calendar days (potential to extend for an additional 45 calendar days for a total of 90 calendar days)
  - "Reasonable data security" still required (though circumstances of pandemic may impact this assessment)

Enforcement Delay for the CCPA?

- Anticipated enforcement as of July 1, 2020 by CA attorney general
- Industry groups have pushed for delay in enforcement given current circumstances
- Consumer advocates have opposed this and encouraged the attorney general to stay the course
- Initial response by attorney general: no delay of enforcement anticipated
- Regulations still yet to be finalized

Thank you!

Questions? Please feel free to contact me any time for guidance.

Elaine F. Harwell
Senior Counsel
Elaine.Harwell@procopio.com
619.906.5780