PUBLICATION

Data Privacy Day: Top Considerations for 2021

Authors: Andrew Jacob Droke
January 28, 2021

Happy Data Privacy Day!

Since 2007, privacy professionals from across the globe have gathered together on January 28 to raise awareness about data privacy and security best practices and issues. The past year presented new challenges and questions for organizations of all sizes, as we responded to enhanced and evolving cyber-attacks; addressed the implementation of new laws and regulations, like the California Consumer Privacy Act (CCPA) and the federal interoperability and information blocking regulations for health care organizations; and developed strategies for responding to new issues related to the COVID-19 pandemic.

As we look forward to 2021, data privacy and security issues will continue to impact businesses of all industries and sizes, and the requirements will affect all aspects of operations.

Key Data Privacy Considerations for 2021:

- **Increased Cyber Attacks:** Organizations must be prepared for increased cyber-attacks after the SolarWinds incident. As data breaches continue to proliferate across all industries, organizations must remain vigilant in protecting both personal information and confidential business information. The Cybersecurity and Infrastructure Security Agency (CISA) recently announced a campaign focused on reducing ransomware and encouraging organizations to implement best practices, tools, and resources. CISA's Joint Ransomware Guide provides helpful resources for mitigating the risks and threats posed by ransomware.

- **Impact on M&A:** Matters regarding data privacy and security will continue to impact M&A activity. As the regulatory framework and risk profile increase in complexity, data privacy and security compliance will be an increasing focus in transactions.

- **Remote Work:** Remote work will continue to evolve and present new questions and challenges for organizations as they adopt and evaluate longer-term considerations for a remote workforce. Biometric privacy requirements are likely to be a critical consideration in this area.

- **New Proposed Privacy Legislation:** With the new administration, we may see federal privacy legislation proposed and passed in 2021. The Biden Administration has already appointed certain key positions, including a position within the Department of Commerce responsible for overseeing the negotiations to create a replacement for the EU-US Privacy Shield that was invalidated in 2020. Given Vice President Harris' prior involvement and interest in California's data privacy and security efforts, we anticipate her close involvement on privacy matters.

- **International Data Transfers:** International data transfers will grow more complex, and data localization requirements will continue to dictate operational data flows and negotiations with technology vendors.

- **Regulatory Changes for Financial Institutions and Health Care Organizations:** Organizations should also anticipate more focused changes on the regulatory front. Financial institutions should expect finalization of GLBA regulations. Health care and health care related organizations should be prepared for additional enforcement and modernization of HIPAA.

While organizations in different industries may experience different impacts in 2021, the implications of new data privacy and security considerations will be widespread. As we prepare for 2021, Baker Donelson's Data Protection, Privacy, and Cybersecurity group continues to anticipate how these evolving issues will impact clients' businesses and to work toward practical solutions in this complex space.

Call to Action: Important Steps to Take in 2021:

- Conduct customized tabletop exercises. This will help refine your incident response plan, as the effectiveness of an incident response team can be significantly diminished without effective training

- Plan strategically for implementing new legislative changes and review your website privacy notices, which are often the most visible aspects of a privacy program. Sign up here to receive our free government relations and public policy alerts and newsletters

- Educate your C-Suite and Board of Directors through a tailored, two-hour data privacy bootcamp covering current data privacy and security issues and include outside counsel and experts for additional context and insights

- Prepare in advance for any acquisition or sale activity including a review of current privacy and security practices and gaps

- Financial institution clients should closely monitor the regulatory environment. See our first webinar in our new series on key data privacy issues for the financial services industry in 2021 here and our alert highlighting 2021 privacy and cybersecurity issues facing financial institutions. Sign up for our Financial Services Transactions list here to receive invitations to future webinars

- Health care clients should stay updated on HIPAA regulations and can sign up for our Health Law and/or Data Protection lists to receive alerts related to HIPAA, interoperability, and information blocking

If you have any questions, or would like to discuss any of the recommended steps above, please feel free to contact Andy Droke or any member of the Data Protection, Privacy, and Cybersecurity Team.