Top Ten Data Privacy Trends for 2021

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Top Ten Data Privacy Trends for 2021

Data continues to be one of the most valuable and targeted resources from organizations of all sizes and across all industries. With the continued state of remote workforces and increased scrutiny on consumer data rights, our team shares what they believe are the top ten data privacy trends to watch for in 2021.

1 The Call for Federal Data Privacy Law Will Gain Momentum

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 which was deemed invalid in 2020.

With Vice President Harris' prior involvement and interest in California's data privacy and security efforts, anticipate her close involvement on privacy matters moving forward.

2 More States Will Introduce or Pass New Data Protection Laws

The momentum of proposed comprehensive state-level privacy laws has never been higher. With the CCPA, CPRA and CDPA passing, additional states have since proposed similar legislation to protect consumers in their own states. Common privacy provisions of the bills that have either passed or have been introduced include:

- Consumer Rights
  - » Right of Access
  - » Right of Rectification
  - » Right of Deletion
  - » Right of Restriction
  - » Right of Portability
  - » Right of Opt-Out
  - » Right Against Automated Decision Making
  - » Private Right of Action
- Business Obligations
  - » Strict Age Opt-in for or Prohibition on Sale of Information
  - » Notice/Transparency Requirement
  - » Data Breach Notification
  - » Risk Assessments
  - » Prohibition on Discrimination (Exercising Rights)
  - » Purpose Limitation
  - » Processing Limitation
  - » Fiduciary Duty

3 Data Privacy Will Become a Bigger Focus in Executive and Board Room Discussions

Boards of Directors have been realizing the importance of strong privacy programs, whether it is a result of hefty fines for violating privacy regulations causing reputational harm or the value-add of building customer trust resulting in the increase of financial benefits, data privacy is becoming more of a priority being driven from the Board.

4 More Companies Will Move to a Single, Enterprise-wide Privacy Strategy

Privacy programs should not operate independently from business strategies, rather privacy strategies should align with information technology strategies, business strategies and the overall mission of the organization.

5 Data Privacy and Cybersecurity Functions Will Become More Integrated

Data Privacy simply doesn't exist without effective cybersecurity. However, just because you have an effective cybersecurity program, that doesn't mean you have an effective data privacy program. Cybersecurity strives to safeguard data, whereas privacy strives to safeguard a person's identity. Therefore, these are not one in the same and rather you need both to be effective in helping protect your organization and its most critical data assets. While good cybersecurity is important, it doesn't address all privacy risks.

6 Third-Party Risk Management Will Continue to be a Major Focus

As we learn of new data and privacy breaches on a weekly basis, a common theme is oftentimes tied to a third-party service provider that exposed the organization. Therefore, it is critical to understand the outsourcing of business functions does not eliminate the risk and threat landscape. Rather, it's only a transfer of risk which needs to be continuously evaluated based on the nature and risk to your organization.

7 A Shortage of Privacy Professionals

Privacy professionals provide a unique value to organizations. Oftentimes an organization's privacy responsibility is placed solely on the Legal team or IT function within an organization. It is critical for organizations to understand their privacy strategy should not only capture the legal requirements, but also how to evaluate the risks posed to the organization and how existing controls or gaps in controls may protect or expose the organization. This is where the IT Risk and Compliance team adds value, as they can help bridge the gap with an understanding of the legal requirements, risk landscape and ability to collaborate with IT to understand the technologies currently in place or those available to help decrease the data footprint, in effort to mitigate the overall risk of unauthorized data exposure. A successful data privacy program leverages the knowledge and skills to ensure collaboration from the Legal, IT Risk and Compliance and IT teams collectively.

8 Employee Training on Data Protection Will Increase

Organizations have done a better job enhancing their cybersecurity awareness training over the years, however is your organization incorporating and differentiating data privacy awareness training? As we mentioned above, cybersecurity isn't enough to ensure an effective data privacy program. It is ever so critical to understand that cybersecurity strives to safeguard data, whereas privacy strives to safeguard a person's identity. Therefore, making sure to incorporate data privacy training into your onboarding and ongoing training awareness programs has never been more critical to help protect an organization's trust, brand, reputation and livelihood, as well as avoid potential heavy fines and penalties.

9 Data Privacy Will Become a Business Differentiator

As data privacy will be one of the most important issues over the next decade, an effective data privacy program can be a business differentiator within your market and industry. By being transparent with your data practices, answering customer concerns up front, along with the ability to show that employees with access to customer data are regularly trained, will collectively help gain and keep customer trust to differentiate your business amongst competitors and in-turn speed up the sales cycle.

10 Significant Increases in Data Subject Access Requests (DSARs) and Complaints

The ongoing push for data privacy regulations globally provides consumers the ability to gain more control over their data. At the same time, consumers are becoming more data aware and want to understand how their personal data is being used and shared among organizations and their third parties. The consumer rights, as mentioned in trend #2 above, allow for the consumer to take back some ownership of their personal data by providing the ability to exercise the right to know, update, delete and even restrict the processing of their personal information. With this, organizations, must have defined procedures in place to record, execute, retain, and log these DSAR requests.

Bonus Trend: More Organizations Will Incorporate Privacy Frameworks

As organizations continue to navigate the ever-changing data privacy landscape, more organizations will start to incorporate privacy frameworks to the help them manage data privacy risks in 2021 and beyond. Leveraging a privacy framework, such as the NIST Privacy Framework, can help organizations create a foundation to build a strong privacy program in effort to ultimately manage privacy risk, while attempting to comply with the evolving data privacy regulations.

About Schneider Downs Data Privacy Services

At Schneider Downs, our IT Risk Advisory Practice has a team of professionals who specialize in data privacy. Our team not only understands the evolving data privacy regulations, but also the technologies that allow for opportunities to enable controls in effort of reducing and protecting the data footprint and ongoing risks of non-compliance.

Ready to Get Started?

For more information on how we can help your data privacy needs please visit www.schneiderdowns.com/data-privacy-services or contact us at contactsd@schneiderdowns.com.

Want to be in the know? Subscribe to our weekly newsletter at www.schneiderdowns.com/subscribe.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com