October 2021

Privacy Compliance Newsletter

Check out ID's Privacy Compliance webpage, where you can find up-to-date thought leadership and download the most recent version of this newsletter.

OCTOBER SPOTLIGHT: WHAT'S LURKING IN THE SHADOWS OF DARK PATTERNS

It's that time of year when pumpkin sales soar, horror movies are plentiful, and everyone plans to dress as some spooky character for trick or treat. It's the tricksters we need to be aware of – the Captain Jack Sparrow type. As a sea pirate, Jack is confident in every situation. He cheats his way through every game and is quick on his feet. He's a thinker and a planner and always two steps ahead of his opponents. His true intentions are known only to him.

Tricksters aren't just for Halloween. You may encounter them daily. Dark patterns are the Jack Sparrow's of website and app design.

What are dark patterns?

Dark patterns are tricks used in websites and apps that cause you to do things you didn't mean to do such as buying something that just showed up in your shopping cart because you selected another item or when you want to unsubscribe from a mailing list but the unsubscribe button is buried in paragraphs of text at the bottom of the page.

Dark patterns aren't just poor UX development, nor are they mistakes. They are carefully planned and executed with an understanding of human psychology...

CONTINUE READING

UPCOMING PRIVACY EVENTS:

TrustWeek – OneTrust User Conference

WHEN: October 12 – 15 | WHERE: Free Virtual Event

TrustWeek brings together OneTrust customers, partners, and industry professionals to learn about the latest technology innovations, share best practices, and network with peers. Take advantage of this free virtal event! **Click here to learn more.**

IAPP Privacy. Security. Risk. 2021

WHEN: October 19 – 22 | WHERE: San Diego, CA

P.S.R. is the number-one event focused on the intersection of privacy and technology. Speakers and breakout sessions will dive deeply into maximizing technology as a privacy asset and minimizing it as a privacy threat. **Click here to learn more.**

PRIVACY HAPPENINGS

PIPL – China's Personal Information Protection Law

China passed PIPL on August 20, 2021, and it takes effect on November 1. Yes, of this year! It's the first comprehensive Chinese law governing how organizations handle the personal information of individuals in China. Its penalties are significant, and some requirements are stricter than those of the GDPR.

Cross-border transfers of personal information are one of its most important restrictions. PI Handlers (like data processors under the GDPR) can only transfer personal information out of China with informed individual consent when necessary for business purposes and after completing a risk assessment. In addition, at least one of the following must be met:

- Passing a security assessment organized by the Cyberspace Administration of China (CAC)
- Obtaining personal information protection certification authorized by the CAC
- Concluding a contract based on a standard contract formulated by the CAC
- Other conditions provided in laws, administrative regulations or by the CAC

There are also stricter controls on the processing of sensitive personal information (SPI). PI Handlers may not process SPI without a specific purpose and must have sufficient need. In addition to typical notice requirements, individuals must be notified why handling their SPI in necessary and how it impacts their personal interests.

Due to the November 1 effective date, organizations should immediately begin reviewing and assessing data processing activities.

Click here to download a more complete PIPL summary

Data Protection Maturity Model Released by CNIL

A data protection maturity self-assessment tool was published by the French data protection authority (CNIL). This maturity model allows organizations to assess their current state against international standards for data protection management. It describes eight typical data protection activities in five maturity levels. After self-assessment, the CNIL expects organizations will be able to create an action plan to fill gaps between their current practices and their targeted maturity levels. The CNIL cautions, however, that the model is not intended to ensure full compliance.

Read the press release and download the model (translation needed).

State Privacy Law Filings Heat Up Yet Again

The 2022 legislative sessions haven't even started, but that hasn't stopped the filing of comprehensive state privacy bills. Oklahoma and Ohio may be the front runners so far.

Oklahoma HB2968 (filed on Sept. 9, 2021) mandates privacy and security requirements for specific types of businesses operating or doing business in OK. It includes the creation and disclosure of privacy policies; limitations on the collection, use and retention of consumer information; and the implementation and maintenance of security procedures, practices, and safeguards. OK residents must opt-in prior to the collection, use, and sale of their personal information. The OK Attorney General is responsible for enforcement. There is no private right of action.

Ohio HB376, Ohio Personal Privacy Act (OPPA), closely resembles Virginia's Consumer Data Protection Act. It applies to businesses conducting business in OH or targeting consumers in the state. OPPA protects personal data of consumers who reside in OH. Employees, contractors, job applicants, officers, directors, and business owners are not considered consumers. The OH Attorney General would have investigative powers and exclusive enforcement authority. The AG must provide a 30-day cure period prior to bringing an action. OPPA also creates a safe harbor for companies complying with the NIST Privacy Framework.

It's heating up to be another busy year along the privacy landscape!

SUBSCRIBE TO FUTURE NEWSLETTERS