2021 Privacy Updates and What It Means for Businesses

In commemoration of Privacy Day this year, we are going to talk about the latest news in privacy and share some tips and resources to help organizations keep current. A lot has happened last year and privacy risks continue to emerge for organizations. As global laws continue to evolve and the US laws play catch up, organizations are drawn to increasing their compliance efforts.

Global Privacy Updates

Let's talk about the elephant in the room, Brexit finally happened. The trade deal between Britain and the European Union has been approved and we are now in the interim "grace period" when data can continue to flow between the EU and the UK in the next four to six months.

To safeguard from data flow interruptions, the following are precautionary measures organization should consider:

- Standard Contractual Clauses (SCC) are reviewed and updated.
- ICO may no longer be a part of GDPR's One Stop Shop, review your interactions with data protection authorities.
- Appoint EU and UK data protection representatives if necessary.
- Update privacy notices, policies and DPIAs (Data Privacy Impact Assessment).

Meanwhile in the southern hemisphere, Brazil's comprehensive privacy law went in effect last September 2020. It's called Lei Geral de Proteção de Dados, or "LGPD". Penalties will take effect in August 2021.

LGPD is heavily inspired by the GDPR and the following are key areas to pay attention to:

- LGDP protects every user in Brazil irrespective of the data subject's nationality and regardless of where the processing agent's company is based.
- Individual rights are consistent with GDPR but in addition, LGPD also gives people a right to access information about those with whom an organization has shared the individual's data.
- Organizations may transfer personal data to other countries that provide an "adequate level of data protection." Brazil has not yet identified which countries it considers as providing an adequate level of protection.

Domestic Privacy Updates

You may already be aware of the California Consumer Privacy Act (CCPA), a pivotal law put into effect last year as the first major privacy law to give American consumers control over their personal information.

Within months of CCPA going into effect, the California Privacy Rights and Enforcement Act (CPRA) was passed this past November and will replace the CCPA as of Jan 1, 2023 - giving businesses two years to revisit their privacy programs to be compliant.

There are key differences between the two - here is a snapshot of a handful of the most notable ones:

- The definition of “business” is shifting and will change the types of business this law will be applicable to. One of these includes the threshold of customers, which will increase from 50,000 to 100,000.
- There is also a new type of personal information defined in the CPRA: Sensitive Personal Information, or SPI. This includes (but is not limited to) passport data, social security numbers, financial account information, race, ethnicity, health records, and union membership.
- New rights will also be set in place, such as right to opt out of automated decision-making technology and right to restrict sensitive PI.

California’s privacy laws have not only impacted businesses everywhere. Many state legislatures around the country are looking to model a similar law as more consumers have demanded transparency over their PII.

The State of Washington, which has numerous times tried to pass a privacy act in the past, is working on a new version for 2021.

This proposal adds stricter protections for consumer data collected during public health emergencies, as well as introduces a private right to action which allows for civil lawsuits in cases for using personal data.

More information around this new Washington Privacy Act will be released as the year goes on, so stay tuned.

Additional Resources

How does one keep abreast of the ever changing regulations? We’ve listed out some resources you can subscribe and follow on.

Organizations should continue to monitor the development of LGPD, the privacy implications of Brexit, and the US State Privacy laws, and are encouraged the following:

- Perform Data Privacy Impact Assessments (DPIA’s) regularly
- Follow the strictest rule applicable to your organization
- Adopt the Privacy By Design Principles (PbD)

If you haven't already checked out these resources, here are some options to get more information on privacy standards.

- NIST
- CIS
- IAPP
- AICPA

Cited Sources:

https://www.dataguidance.com/sites/default/files/gdpr_lgpd_report.pdf
https://iapp.org/resources/article/state-comparison-table/
https://www.jdsupra.com/legalnews/third-time-could-be-the-charm-for-20529/
https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed