ARTICLE

Streamlining privacy compliance among global regulatory changes

Organisations that operate globally are subject to the ever-changing and constantly developing regulatory landscape. This remains a challenge for all industry sectors.

In the wake of a year with pivotal change and extreme reliance on the internet and e-commerce, it is hardly surprising that regulatory activity is increasing on a global scale. New technologies have helped expand and globalise markets, making products developed and marketed in one corner of the world available for purchase and delivery across virtually any border. But playing in many leagues means playing by many rules. And these rules tend to change often. When building products and providing services in a particular geographical location, organisations must know what rules to follow and be prepared to respond when regulators come asking about their practices.

Challenges

Privacy rules and guidelines are developing worldwide, and many organisations have felt the challenge of adapting to these changes. The IAPP Privacy Risk study of 2020 found that "even industries structured for regulatory compliance, such as the financial services and health/pharma industry sectors, see privacy law compliance as at least a short-term business risk due to the global variance in privacy laws." Big tech also experienced significant changes with the Digital Services Act, and the Digital Markets Act brought forward in the EU to create a safer and open digital market.

Moving Forward

Navigating the changing regulatory landscape and achieving a mature level of compliance for those regions will require consideration of several factors, including:

1. **Data mapping.** Some organisations paused compliance efforts because of the pandemic or changes in corporate priorities. In 2020, GDPR penalties reached $193million, a 39% jump from the prior year. Waiting is not a viable option. Organisations need to understand and document the personal data they process, where it flows, to whom it is disclosed, and which vendors are used. The earlier an organisation maps these data flows and practices, the easier it will be to manage, adapt and comply with changing and multi-jurisdictional privacy rules.
2. **Data transfers**. Any organisation using a system, vendor or otherwise intending on exporting EU personal data outside Europe, may need to take additional measures to avoid running afoul of the latest developments. With the Brexit transition period now complete, data flows between the EU and the U.K. are a serious consideration. Developments in this area are constantly evolving, so it's critical to keep a close eye on regulatory developments.

3. **Consent**. Organisations that rely on consent to process personal data will need to make sure they can demonstrate that data subjects are informed and freely gave the consent through a clear, specific, and affirmative action. They must be informed through easy to understand and accessible means that enable the individual to withdraw consent at any time. Websites must obtain and store cookie consent from EU visitors. Multiple EU Data Protection Authorities have indicated more vigorous enforcement on cookie compliance moving forward. In 2020, two U.S.-based tech firms were fined €135million for alleged cookie violations.
4. **Data subject requests (DSRs).** The GDPR gives a set of rights to individuals to be able to access, modify, delete or export their personal data. Organisations need to have the means to support DSR requests, validate the individual's identity, search for the data and perform supplemental actions where required, and fulfil these requests within one month.
5. **Breach preparedness.** In the event of a breach where personal data is lost, stolen or unavailable, organisations may need to notify the data protection authority within 72 hours of awareness. In certain instances, organisations must also notify data subjects. While most organisations are focused on improving cyber controls, they must be prepared for the privacy considerations and obligations in the event of EU personal data being breached.
6. **Privacy operations.** When privacy legislation or practices change in a jurisdiction where your organisation operates, you want to be the first to know, and you want to take action as soon as possible. This is easier for compliance professionals when their privacy programme is supported by privacy management software through which templates can be built, progress can be tracked, and information is preserved, giving a holistic view of risks.

According to the recently published IAPP-FTI Consulting Privacy Governance Report 2020, between 96% and 98% of privacy teams' top responsibilities are "Privacy policies, procedures and governance," "Following legislative developments around privacy and data protection" and "Addressing privacy issues with existing products and services." However, only 68% of respondents see "Acquiring and/or using privacy-enhancing software" as their responsibility. When compliance is built with standalone, static documents, changes and updates become cumbersome and difficult to implement. Technology can support mapping exercises with visual aids and connecting data points and sources with compliance activities such as access requests and data protection impact assessments (DPIAs).

7. **Contextualise privacy**. It is essential to ensure privacy is woven into the fabric of each stakeholder's workflow. Teams across the organization will need to have privacy in mind, often considering what effect, if any, a particular action in service delivery or a functionality in a product will have on a user's privacy rights.

Conclusion

Organisations that operate globally are subject to the ever-changing and continually developing regulatory landscape, which is challenging to comply with without a robust privacy and information governance backbone. Using aids such as privacy management technology to stay on top of processing activities and legal requirements will facilitate compliance teams' work and serve as the go-to resource for updates, queries, and research on regulatory changes.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

INÉS RUBIO
+353 860 521789
ines.rubio@fticonsulting.com