GDPR – YEAR ONE: PRACTITIONERS' PERSPECTIVE

By Dawn Newton & Shruti Bhutani Arora

May 25th marks the first anniversary of the enforcement of the European Union's General Data Protection Agreement (GDPR). GDPR has ushered in a new era of data privacy and security laws and compliance. Several jurisdictions, such as California, Brazil, China, India, Japan, South Korea, and Thailand have passed new laws, proposed new legislation, or are considering changes to existing laws that will bring their privacy laws into closer alignment with GDPR. Even the U.S. Congress is in the very early stages of contemplating federal data privacy legislation.

According to the International Association of Privacy Professionals, over the last year in the EU, more than 94,000 individual complaints have been filed, 200,000 cases have been received by Data Protection Authorities, and GDPR enforcement actions have resulted in over €56,000,000 in fines.[1]

There is little question that data privacy and security has become a hot topic, which shows no sign of slowing down. If anything, compliance obligations are only increasing with evidence that enforcement actions are abundant, and more jurisdictions are imposing their own laws.

So what have we observed in the past year while helping clients with their GDPR compliance?

1. Privacy Shield Certification Delays.
Our clients have faced delays in getting self-certified to the EU-U.S and Swiss-U.S. Privacy Shield Frameworks because of the immense volume of application received by the International Trade Administration (ITA) within the U.S. Department of Commerce that administers the Privacy Shield Frameworks. Privacy Shield certification allows a business to transmit data from the EU and Switzerland to the U.S., so self-certification has been in high demand. Therefore, if you are looking to self-certify to the EU-U.S. and/or Swiss-U.S. Privacy Shield Frameworks, it is best to start early.

2. Consumer Concerns.
This past year businesses have also received inquiries by individuals about how businesses have obtained their email addresses, how their consent is recorded, and how their data is stored, transmitted, and used. These inquiries are coming from both European residents and residents of other countries. Individuals increasingly care about the privacy, security, and communication practices of the businesses they patronize.

3. DPA Negotiations.
A Data Processing Agreement (DPA) is the agreement between two businesses which allows one to use the other as a vendor reliably, with assurances that the vendor will comply with GDPR and not engage in behavior which puts the hiring business at risk. While some businesses have viewed these as boilerplate - a nuisance to simply sign and put in a drawer - they can have many significant terms which are worth evaluating. We have negotiated the timeline for reporting breaches, the scope of audit rights in a DPA, managing data during the audit, and the party responsible for paying for audits. For significant relationships, it can be well worth the time to evaluate whether the DPA should be reviewed and revised.

4. Internal Policies and Training.
Once the mad rush to update external-facing documents like privacy policies and websites by May 25, 2018, ended, companies had an opportunity to make sure their internal practices were fully in line. We saw an increased shift towards businesses having internal policies on data collection, retention, deletion, and data breach, and training their employees on those policies. This is an important step because such training determines how a company identifies, reacts, and reports data breaches. It is particularly important to understand that a Data Protection Authority will take this type of internal documentation and training into consideration if it is reviewing a complaint against a business. The best case scenario is to prevent problems from occurring, but if a problem has occurred and the business is being investigated, you will be glad to have records of internal compliance policies and education.

What can we expect in the coming year?

According to Helen Dixon, Data Protection Commissioner for Ireland, speaking at the International Association of Privacy Professionals Global Summit which we attended, this summer we are likely to see "first-draft decisions" on GDPR violations involving large data breaches, systemic privacy issues and other serious violations at technology firms. She also said that "GDPR really looks into the behavior, on the one side, of the company, and on the other side, the infringement and how we can deal with that. It's important to know the proportionality principle doesn't only deal with big companies but also small companies."

In the coming year, we anticipate increased GDPR enforcement on small- and mid-sized companies. Data privacy and security is going to become, if it is already not, one of the significant compliance issues for any company that electronically collects, stores, and processes data.

For businesses which have struggled with how to prioritize compliance amid many other needs, while the so-called "grace period" for compliance is over, you have not necessarily missed the boat. Starting compliance efforts now can help show efforts to comply with GDPR which will be viewed favorably when compared to no effort to comply. Come talk to us for perspectives on how to start "bite-sized" compliance, avoid red flags which may make your business more likely to be targeted, and the coming California Consumer Protection Act which will bring a new version of privacy rights to California residents starting January 1, 2020.

[1] https://iapp.org/resources/article/gdpr-one-year-anniversary-infographic/

Dawn Newton
Partner
dnewton@donahue.com

Shruti Bhutani Arora
Associate
sarora@donahue.com

DONAHUE FITZGERALD ATTORNEYS