GDPR ONE YEAR LATER:

A DATA PRIVACY RETROSPECTIVE

Long part of social and corporate consciousness in the European Union (EU), data privacy is now a household topic in the US. Seemingly every day we hear about a company venturing to store more of our personal information to provide a better user experience. While this may provide individuals with enhanced information at their fingertips, companies are struggling to implement the required data privacy compliance regimes. Privacy compliance is costing companies millions of dollars as they implement new practices, policies, and procedures. Some organizations are struggling to keep up, shifting personnel from their day-to-day roles and responsibilities to address privacy. Privacy breaches have elevated data privacy awareness to a new level. Regulations like the EU's General Data Protection Regulation (GDPR), the Personal Information Protection and Electronic Documents Act (PIPEDA), the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Rule (COPPA), and China and Brazil's new data privacy laws have been drafted and enacted over the last several years to better protect individual rights.

BDO

ONE YEAR AFTER GDPR

On May 25, 2018 the EU's GDPR went into effect. This was, by far, the most aggressive and sweeping privacy law the world had seen in years. New requirements including: a) responding to individual rights requests within 30 days unless certain criteria are met, and b) filing with regulators within 72 hours of a personal data breach, were just a couple of the most pressing obligations companies are required to address.

Over the last year, fines have been wide ranging and have varied from country to country. Companies of all sizes across different industries have been caught in the cross-hairs of the regulators, including but not limited to:

Knuddels.de

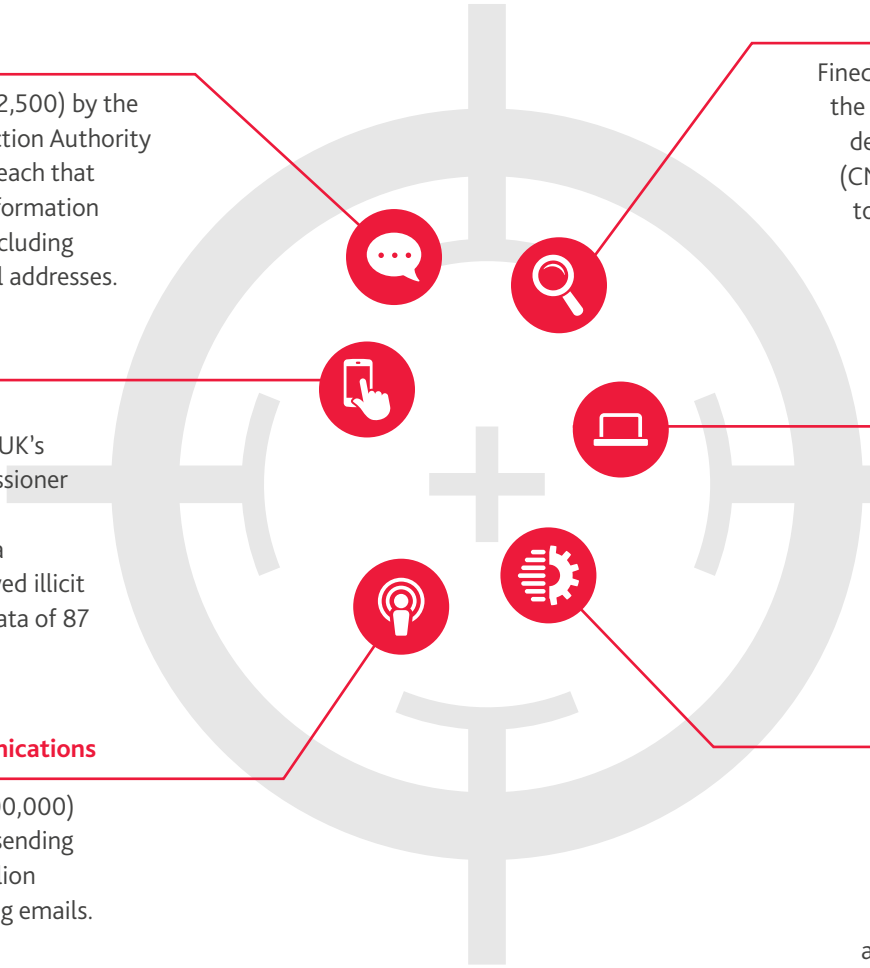
Fined €20,000 (~$22,500) by the German Data Protection Authority (DPA) following a breach that exposed personal information of 330,000 users, including passwords and email addresses.

Facebook

Fined £500,000 (~$652,000) by the UK's Information Commissioner Office (ICO) for the Cambridge Analytica scandal, which allowed illicit access to personal data of 87 million users.

British Telecommunications

Fined £77,000 (~$100,000) by the UK's ICO for sending approximately 5 million unsolicited marketing emails.



Google

Fined €50 million (~$57 million) by the French Commission Nationale de l'informatique et des Libertés (CNIL) for not properly disclosing to users how data was collected across its services to provide personalized advertisements.

Yahoo!

Fined £250,000 ($326,000) by the UK's ICO for an attack that took place in 2014 where contact information and passwords of 500 million users were exposed.

Equifax

Fined £500,000 (~$652,000) by the UK's ICO for a 2017 breach that allowed hackers to steal sensitive financial information from approximately 15 million users.

In response to these fines, companies are taking action to improve their data governance and privacy compliance programs. In the last year, we have seen more companies take action to:

- Identify and map data sources, whether in-house or external to their operations;
- Operationalize privacy policies to drive employee compliance and enforce non-compliance;
- Gather documentation to update and maintain data registers, logging information about processes and systems that store personal and sensitive information;
- Train employees regarding their responsibility to protect personal information; and,
- Restructure data retention and classification capabilities by updating records retention schedules, developing more stringent data disposition practices, and developing/updating data classification programs.

Although these practices are table stakes for sound data governance programs, companies have historically put data governance on the back burner. GDPR changed that. And, if your company operates in California and has gross revenues in excess of $25 million; OR buys, receives, sells, or shares the personal information of more than 50,000 or more consumers; OR derives 50% or more of business from selling personal information, addressing data governance and privacy compliance is now even more critical.

CCPA GOES INTO EFFECT JANUARY 1, 2020

Companies seem to be taking a less aggressive approach in their CCPA preparations than they did with GDPR. However, this approach presents a host of potential issues and complexities as companies contemplate their CCPA posture and subsequently their CCPA compliance budgets. Although CCPA will be effective January 1, 2020, consumers will have the ability to request a 12-month lookback. In other words, this lookback provides the consumer with the right to access their personal information for the past 12 months. Information that may be requested includes:

- Categories of personal information collected about the consumer, as well as categories of sources from which the personal information is collected;
- Specific personal information collected about the consumer;
- The commercial reason(s) why a business collects or sells the personal information;
- Categories of third parties in which the business shares personal information;
- Categories of consumers' personal information that is sold to various categories of third parties (note, the CCPA defines "sell," "selling," "sale," or "sold" very broadly); and
- Categories of consumers' personal information that is disclosed for a business purpose.

To comply with these requests, companies need to understand where the personal information of their customers resides, either on their systems or potentially with third parties. While this sounds like a relatively simple process, it can be one of the most challenging tasks for companies to accomplish, due in large part to the concept of Big Data. To institute good data discovery and mapping practices, follow these five steps:

1. Obtain copies of system and data inventories, if they exist, and identify where updates are required;
2. Interview teams primarily responsible for interacting with particular types of data;
3. Consult with service providers integral to the operations or management of data;
4. Understand all types of data that may be available, including metadata, geolocation data, and IP addresses, to fully understand what information is available; and,
5. Document updated inventories and data flow diagrams.

Compliance with the CCPA starts with good records management practices – an often forgotten discipline. Here are other steps to consider:

Evaluate data governance and privacy maturity
Conduct an assessment to understand the current state of your privacy program; during the assessment, identify gaps and resource needs, and define a roadmap to readiness.

Create a data inventory
A data inventory and data flow diagrams will provide insight into the locations of your data, who can access it, how it is protected, and what information is available for consumers to request.

Integrate your GDPR individual rights response program with your CCPA consumer rights management program
If you did not yet institute a GDPR individual rights response program, it is now time to establish a CCPA consumer rights management program, and integrate the two. First, consider teams currently in place who manage customer requests or provide help desk support; the necessary infrastructure may reside within those teams. Then, consider the staff and whether they have capacity or the ability to respond to and track consumer requests. If not, consider additional resources, both technology and personnel.

Train your team members and develop a privacy awareness program
The concepts and tools within data governance and privacy programs need to be regularly communicated to your team to drive compliance with their obligations.

Consider your online presence and related policies
Online privacy policies and notices should match actual practices. The online notices and policies should include your CCPA practices, how customers will be able to access their information, and provide an online opt-out mechanism for consumers.

While there are a number of considerations when instituting sound data governance and privacy compliance practices, the items mentioned in this article provide a good starting point. CCPA fines could be $2,500 per violation and up to $7,500 per intentional violation before law suits are filed. Remember to keep alert for additions or amendments to the CCPA as it becomes effective in January 2020.

CONTACTS:

KAREN SCHULER
Principal, National Governance & Compliance Leader
703-336-1533
kschuler@bdo.com

MARK ANTALIK
Managing Director,
Information Governance Leader
617-378-3653
mantalik@bdo.com

SANGEET RAJAN
Managing Director,
Governance & Compliance
415-490-3001
srajan@bdo.com