Three Things: The Future of Privacy Legislation

By Naveed Cheraghchi & Brian J. Reilly

With the start of the New Year comes the enforcement of one of the country's most anticipated pieces of legislation, the California Consumer Privacy Act (CCPA). In many ways, the CCPA is similar to its European counterpart, the General Data Protection Regulation (GDPR). This edition of *Three Things* provides a reminder of what businesses can do now to begin the process of complying with both the CCPA and GDPR.

1. DATA COLLECTION Both CCPA and GDPR restrict the collection of data that can be traced back to the individual, known as personal data/information. To be subject to the CCPA, a company must do business in California and meet at least one of three criteria: (1) have a gross revenue greater than $25 million; (2) annually buy, receive, sell, or share the personal information of more than 50,000 California residents, households, or devices for commercial purposes; or (3) derive 50 percent or more of its annual revenue from selling California residents' personal information. The GDPR applies to data controllers and processors that are (1) established in the EU and process personal data in the context of their activities, regardless of whether the processing takes place in the EU; or (2) not established in the EU that process personal data in connection with offering goods or services in the EU, or monitoring their behavior. Regulated businesses must aggregate or anonymize data so that consumers can't be identified through the collected information. Additionally, the regulations require businesses to inform consumers what kind of data is being collected and the purposes for the collection.

Action: Businesses should conduct a data inventory of all of the personal information that they collect and ensure that data is unidentifiable.

2. DATA PROTECTION Neither CCPA nor GDPR states the specific security measures that must be implemented by companies. Instead, the CCPA establishes a way for consumers to sue companies for data breaches when the companies don't meet their duty to implement and maintain reasonable security practices, and the GDPR requires businesses to take measures proportional to the security risks. Importantly, consumers have a right of access under both the CCPA and GDPR, which means businesses must be able to inform consumers exactly what information the business has collected, and how that information is being processed. Businesses must also be aware that consumers have a right to opt-out. Under the CCPA, consumers have an absolute right to opt-out of the sale of their personal data. The GDPR has an exception from opting-out if there are legitimate grounds for the data processing, but otherwise consumers can opt out of any processing of their data, not just its sale.

Action: Businesses must ensure that they have written contracts with any service providers they may share the data with. If not, they could face penalties if the service provider fails to comply with the applicable regulation. Businesses should also update their privacy policies and procedures with these data protection standards in mind; in Massachusetts, this includes implementing and abiding by a written information security policy.

3. DISPOSAL OF DATA Businesses must also be wary of consumers' right to deletion under both the CCPA and GDPR. The CCPA's right to deletion is broad, but subject to a few exceptions. Under the GDPR, consumers can request deletion only if the request meets one of six criteria. Both the CCPA and GDPR also require businesses to instruct downstream data recipients to delete the data as well.

Action: To meet these requirements, businesses should implement a consumer self-service model to assist in handling deletion requests. The same model could also be used to facilitate right of access and opt-out requests.

Date Created
December 17, 2019