THE FUTURE OF DATA SECURITY FOR EMPLOYERS
GLOBAL TRENDS IN DATA PRIVACY REGULATION

RISA BOERNER (CIPP/US) (PHILADELPHIA)
DANIELLE URBAN (CIPP/E) (DENVER)
FISHER PHILLIPS LLP

I. Introduction

Over the course of the last several years, news reports of major data breaches have become increasingly frequent. Data breaches across the globe have drawn widespread attention, largely due to the fact that entities of all sizes have transitioned to reliance on digital storage of personal data, in the cloud and otherwise, to manage the vast amounts of personal data collected from consumers and employees. Beginning most notably with the widely publicized 2013 Target data breach that exposed the credit and debit card data of up to 40 million consumers, news reports of major data breaches have become almost commonplace.

Privacy regulations, which for many years were either lax or non-existent, have finally begun to recognize and address the tremendous risks inherent in the collection and storage of sensitive personal data. In the past year, in particular, we have witnessed significant changes in data privacy regulation, both in the United States and abroad. The European Union's General Data Protection Regulation (GDPR) went into effect in May 2018, two years after its initial publication in the Official Journal of the European Union. The GDPR contains sweeping reforms, and has caused many businesses to reevaluate the manner in which they maintain and use both consumer and employee personal data. It carries the potential for crippling fines for noncompliance.

Just one month after the implementation of GDPR, in June 2018, California passed the California Consumer Protection Act (CCPA), with an implementation date of January 2020. The CCPA is arguably the most ambitious and far-ranging privacy regulation enacted to date in the United States, and it borrows heavily from the GDPR in terms of the protection it provides to individuals with respect to the collection and use of their personal information.

The GDPR and CCPA, together with other laws and regulations passed by countries across the globe, reflect a changing tide in data protection that is likely to continue in 2019 and beyond. The new trend limits businesses' ability to collect, maintain, and use individuals' personal data without proper notice and consent, and affords individuals greater rights to obtain, delete, and revise inaccurate personal information that has been collected. This white paper will take a closer look at global trends in data privacy regulations, with an emphasis on GDPR and CCPA, and will offer recommendations for how companies can prepare now for changes that are likely to occur in 2019 and beyond.

II. The GDPR

The GDPR expands individuals' rights to control their personal data, imposing restrictions on the collection, use, and maintenance of data, as well as new notification requirements in the event of a data breach. Penalties for non-compliance can be as high as 4 percent of global turnover or 20 million Euro, whichever is higher. Guidance issued by the Article 29 Data Protection Working Authority several months before the law became effective emphasized the goal of achieving consistency in enforcement of the GDPR – including the imposition of fines – among the supervisory authorities in the European Union.[1] Generally, penalties for non-compliance are to be imposed on a case-by-case basis and are intended to be "effective, proportionate, and dissuasive."

Companies have been watching closely for indications of how the GDPR will be enforced and whether and when maximum fines will be assessed. Enforcement notices and penalties have been issued, providing a preliminary idea of how violations are likely to be treated going forward.

[1] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017.

This section contains an overview of the GDPR's requirements and a summary and analysis of enforcement actions to date.

A. Overview

1. Application Of The GDPR

Under Article 3 of the GDPR, if your company collects personal or behavioral information from an EU resident, your company is subject to the requirements of the GDPR. The law only applies if the data subjects are in the EU when the data is collected. "Personal data" is defined as "any information relating to an identified or identifiable natural person ('data subject')," and includes personal identification information such as name, email, address, and ID numbers; web data, including location, IP address, cookies data, and RFID tags; health, genetic, and biometric data; race or ethnic data; political opinions; and, sexual orientation.

The GDPR applies to controllers and processors of personal data. A data controller owns the data, and must have legal agreements in place with data processors, who will process the data on behalf of the controller. The data processor has no ownership rights to the data, and must delete the data when the processing is finished. Under the GDPR, personal data can be processed only if there is a legal basis for the processing. The legal bases for processing data include:

1. The data subject has given consent to the processing of his/her personal data for one or more specific purposes;

2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

3. Processing is necessary for compliance with a legal obligation to which the controller is subject;

4. Processing is necessary in order to protect the vital interests of the data subject;

5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and

6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The data controller is responsible for informing data subjects of the legal basis for processing the subject's data, and obtaining permission to do so. Data subjects must be notified of the legal basis for processing data at the outset, grant permission to the controller to process information, and be notified anytime the legal basis for processing changes.

2. Key Provisions

a. Consent

Data subjects must give their consent to have their data processed, and consent must be "freely given, specific, informed, and unambiguous." This means that data controllers must provide subjects with notices outlining, among other requirements, how the data will be used, the legal basis for processing, how the data will be stored, who will have access to the data, and how long the data will be kept. Under the GDPR, it is not permissible to hold data indefinitely or to hold data not necessary for processing a particular transaction.

b. Breach Notification

In the event of a data breach that is likely to result in the unauthorized use or distribution of data, data controllers must notify data subjects within 72 hours of becoming aware of the breach, making it important for data controllers to understand exactly what happened and who was affected by the breach. There is an exception to breach notification if the breach involved encrypted data and the means to decrypt was not stolen or compromised. Data processors have the same time frame in which to notify data controllers of any breach.

c. Right To Access

GDPR requires that data subjects be informed regarding how, where and for what purpose their personal data is being processed, typically in the form of a clear and conspicuous privacy notice.

d. Right To Be Forgotten

Data subjects have the right to request that their personal data be deleted, and the right to demand that the processing of their personal data be stopped and no longer used by third parties.

e. Data Portability

Data subjects also have the right to receive their personal data in a machine-readable format and to have their personal data transmitted to another controller.

f. Privacy By Design

Privacy by design requires that companies take data privacy into account when designing data processing systems. Data controllers must also take steps to limit the access of personal data to only those individuals who need the data to complete their processing duties. The controllers should hold and process only the data absolutely necessary for the completion of its processing duties, as well as limiting access to the personal data

B. GDPR Enforcement To Date

In the short time that has elapsed since the implementation of the GDPR, the European Union data protection authorities have received more than 95,000 complaints.[2] This began on the very first day the law went into effect. On that day, a consumer rights group filed a complaint against Facebook, Google, Instagram, and What's App, claiming that all four services violated the

[2] European Commission Press Release, 25 January 2019, available at: http://europa.eu/rapid/press-release_STATEMENT-19-662_en.htm.

GDPR by employing a strategy of "forced consent" to continue processing users' personal data. That complaint is still pending, but others have since been decided.

1. Fines Issued By EU Data Protection Authorities

Four fines are known to have been issued to date for GDPR violations. They include the following:

- Austria: In October 2018, the Austrian data protection authority issued a fine against a betting shop that had installed security cameras to record part of the pavement outside the shop. The GDPR prohibits large-scale monitoring of public spaces. The fine imposed for this violation was 4,800 Euro.

- Portugal: Also in October 2018, the Portuguese Supervisory Authority imposed fines totaling 400,000 Euro on a hospital for GDPR violations relating to the processing and storage of personal data. After investigation, it was determined that hospital staff members had illicitly accessed patient data through false profiles. The hospital had only 296 registered doctors, but the profile management system listed 985 physicians with active accounts giving them unrestricted access to all patient profiles, regardless of specialty. The supervisory authority concluded that the hospital had not implemented appropriate technical and organizational measures to protect patent data. The hospital reportedly claimed that its processes were adequate because it used the IT system provided to public hospitals by the Portuguese Health Ministry. The supervisory authority rejected this claim, finding that it was the hospital's responsibility to ensure that the IT system complied with the GDPR. The hospital is contesting the fine.

- Germany: In November 2018, the German data protection supervisory authority for the German state of Baden-Württemberg imposed a 20,000 Euro fine on a German social network, Kuddels.de, after a cyberattack that reportedly caused over 800,000 email addresses to be leaked, together with 1.8 million usernames and passwords. A portion of the information was then published online without any encryption. The social network claimed that once the leak was discovered, it immediately improved its security measures.

  The German data protection authority that issued the fine said that one of the reasons the website received a "relatively low" fine was the company's "exemplary" cooperation with the authorities and its transparency, by disclosing its shortcomings, and be willingly implementing the authority's instructions and recommendations. The authority also took into account the overall financial burden for the company in implementing the new security measures, which amounted to a six-digit figure. In a statement, the authority said: "[a]s data protection authority, it is not [our] aim … to compete for the highest possible

fines. What really matters is the improvement of the level of data protection and data security for the users concerned."

- France: The most recent fine issued in response to GDPR violations was also the largest: 50 million Euro, against Google. The January 2019 fine, issued by the French data protection authority, was in response to Google's alleged failure to provide users with transparent and understandable information on its data use policies. Specifically, the DPA investigated the Android's user "click path" from the creation of a Google account to the day-to-day use of the smartphone and concluded that Google was in violation of two of the GDPR's main principles: (1) lack of transparency and inadequate information; and (2) lack of valid consent regarding the ads' personalization. Among other things, the French data protection authority noted that Google users are asked to tick the boxes "I agree to Google's Terms of Service" and "I agree to the processing of my information as described above and further explained in the Privacy Policy" in order to create a Google account. This method of securing consent was deemed to be inappropriate because it was "bundled." In issuing the 50 million Euro fine, which while large was far from the maximum potential fine of 4 percent global turnover, the French data protection authority explained that the fine and publicity of the decision were justified by "the severity of the infringements observed regarding the essential principles of the GDPR: transparency, information and consent."

2. Observations Based On Fines To Date

Based on the fines issued to date, to the extent the decisions can be harmonized, it appears that the data protection authorities are placing a premium on transparency and cooperation, and taking into account the severity of the violation, as well as a company's willingness to quickly implement appropriate measures to comply with the GDPR. Based on the Austrian data protection authority's betting shop fine, it also appears that the authorities are intent on enforcing the GDPR not only against large global conglomerates, but also smaller businesses.

Even Google's recent fine, while large, is not close to the maximum possible fine, suggesting that although the data protection authorities are likely to issue fines for violations that are perceived to be significant, they are not determined to impose the most serious fines in all possible situations, possibly reserving them for the most egregious matters and a demonstrated

unwillingness to cooperate, or repeat violations that reflect an indifference to the requirements of the GDPR.

III. The California Consumer Protection Act

In June 2018, one month after the GDPR took effect, California passed the CCPA. The CCPA is a first-of-its-kind law in the United States, borrowing heavily from the principles of the GDPR, and placing an emphasis on individuals' right to control the dissemination and use of their personal data. The CCPA was hastily introduced and passed as a compromise to prevent an even stricter initiative from appearing on the November 2018 ballot.

The CCPA has already been amended once, and further amendments are expected following a series of public forums held by the California Attorney General in early 2019 seeking public comment on the CCPA. The law's current effective date is January 1, 2020, although the initial amendments to the bill preclude the Attorney General from bringing an enforcement action under the CCPA until the earlier of six months after final regulations are published implementing the provisions of the CCPA, and July 1, 2020.

A. Overview Of The CCPA

In general terms, the CCPA allows California residents to request that businesses disclose the information they are collecting, the source of the information collected, and with whom the information is shared. The CCPA also permits individuals to opt out of the sale of their personal information, and prohibits businesses from discriminating against those who exercise their rights under the law.

The CCPA applies to businesses that:

(1) are for profit;

(2) collect consumers' personal information (as defined by the CCPA), or on behalf of which such information is collected;

(3) determine the purposes and means of processing of consumers' personal information; and

(4) do business in California, while
   a. having an annual gross revenue of over $25 million;
   b. buying/selling or receiving/sharing for "commercial purposes" the data of 50,000 California residents; or
   c. deriving 50 percent of their revenue from "selling" the personal data of California residents.

The CCPA also applies to any entity that controls or is controlled by the business (i.e. parent companies and subsidiaries). Although the CCPA is a "consumer" protection act, the Act is broad enough to include employee data. The breadth of the law is reflected in the definition of "consumer," which includes any "natural person who is a California resident," as well as the definition of the term "personal information," which is expressly defined to include "employment-related information."

B. Comparison Of The CCPA To The GDPR

There are many similarities between the GDPR and the CCPA, but the laws are not identical, and at present, the CCPA does not contain any provisions exempting companies that are in compliance with the GDPR from compliance with the CCPA. This has caused confusion and some concern from companies that have spent years and invested significant financial resources bringing their data into compliance with the GDPR. This issue has been raised at the public forums referenced above, and it is as yet unclear whether the law will be amended to include a safe harbor for companies that comply with GDPR requirements.

The following is a list of some of the key similarities and differences between the CCPA and GDPR:

- **Key Differences:**

- Who is regulated: The GDPR is broader in application than the CCPA. The GDPR applies to "data controllers and data processors" (1) established in the European Union that process personal data in the context of activities of the European Union establishment, regardless of whether the data processing takes place in the European Union; and (2) not established in the European Union that process European Union data subjects' personal data in connection with offering goods and services in the European Union, or monitoring their behavior. The CCPA applies to a narrower category of businesses, as explained in greater detail above.

- Children: The CCPA only requires parental consent for personal data sales; GDPR's parental consent requirement applies to all processing consent requests.

- Right of recertification (*i.e.* the right to correct incorrect data): The GDPR permits individuals to request correction of inaccurate data. The CCPA does not contain a similar provision.

- Right to object to processing of data: The CCPA contains no such restriction, other than the right to opt-out of the sale of personal information. By contrast, the GDPR contains a right to object to processing for profiling, direct marketing, and statistical, scientific, or historical research purposes.

- Right to object to automated decision making: The GDPR restricts companies' ability to make decisions based solely on automated processing of data. The CCPA does not.

- Penalties for noncompliance: As noted above, the GDPR permits the imposition of maximum fines of up to 4 percent of global turnover, or 20 million Euro, whichever is greater. Under the CCPA, the California Attorney General can bring actions for civil penalties of $2,500 per violation or up to $7,500 per violation if the violation is intentional. The CCPA, unlike the GDPR, grants businesses a 30-day cure period for violations. The CCPA also permits a narrow private right of action for certain data breaches involving a subset of personal information. However, the CCPA also grants a 30-day period to cure such violations, if possible.

- **Key Similarities:**

  - Who is protected. This is defined differently in the two laws, but the effect is similar. Both focus on information that relates to an identifiable natural person. Both also have potential extraterritorial effects that businesses outside the jurisdiction must consider.

  - What information is protected. This, too, is similar, although the CCPA's definitions also include information linked at the household or device level. The GDPR defines personal data as any information relating to an identified or identifiable data subject.

- Anonymous, deidentified, pseudonymous, or aggregated data: The laws are similar in their application to such data. Both require technical controls to prevent re-identification.

- Rights of Disclosure/Access. The CCPA's right is only to obtain a written disclosure of information collected by the business. The GDPR allows broader access, which is not limited to a written disclosure in a portable format.

- Right to deletion. Both laws permit individuals to request deletion of their personal data, although the CCPA contains more bases to refuse the request.

- Privacy notices. The two laws contain similar disclosure requirements, but there are differences in the specific information delivery methods required.

C. What Companies Can Do To Prepare Now For The CCPA

Businesses should take note of several important provisions that will require preparation prior to the CCPA's January 1, 2020 effective date. They include:

- Update Privacy Notices: At or before the time of collecting personal information, businesses must provide notice of the categories of personal information to be collected, and the purposes for which they will be used.

- Identify Personal Information in the Company's Possession and Create Strategies for Complying with Consumer Requests: The CCPA requires businesses to disclose certain categories of personal information they collect regarding consumers, including categories and specific pieces of consumer information that has been collected, the sources from which the information is collected, the purposes for collecting or selling personal information, and categories of third parties with whom the business shares personal information. Additionally, at a consumer's request, businesses must deliver all personal information collected regarding the individual, and businesses must also delete personal information at the request of the consumer (with certain exceptions). In order to be able to comply with these requirements, businesses must know what type of data they collect, and they must have procedures in place to respond to consumers' requests in a timely fashion.

- Non-Discrimination: With some exceptions, businesses cannot discriminate against an individual simply because the individual exercised their rights under the CCPA, including denying goods or services, charging different prices, providing a different level of quality of goods or services, or suggesting that the individual will receive a different price or level of quality of goods or services. It is important that companies review their policies and procedures to ensure

that they are not inadvertently violating this obligation by denying certain goods or services to individuals for exercising rights guaranteed by the CCPA.

The CCPA will almost certainly be amended at least one more time before its implementation date, but companies should consider beginning to review their policies and procedures now to ensure that they will be in compliance with the CCPA's key provisions when they take effect.

IV. Pending Legislation And Likely Trends In Data Protection

In January 2019, the Washington state senate passed the Washington Privacy Act, a sweeping privacy law similar in scope to the CCPA, and borrowing heavily from GDPR as well. It presently remains to be seen whether the legislation will pass and become law, but it marks a significant development, suggesting that state legislatures are taking note of the global trend in enhanced protection of personal information, and looking for opportunities to remain in step with that trend.

State legislatures have been broadening existing protections for personal information through amendment and expansion of existing data breach notification laws for some time, expanding the definition of "personally identifiable information" to include more categories of information, and tightening requirements for breach notification, as well as implementing new requirements for safeguarding personal information protected by these statutes. The CCPA and the proposed Washington legislation go further, providing enhanced notice and consent provisions. This trend is likely to continue.

At the federal level, several privacy bills have been introduced in the last year, including the Data Care Act, proposed by 15 Democratic senators in December 2018, as well as the Consumer Data Protection Act, introduced in November 2018 by Democrat Ron Wyden (D-Ore.), which would impose stringent penalties for non-compliance, among others. Some of the

bills borrow from the GDPR and CCPA, while others focus more narrowly on specific industries and issues.

Although it is as yet unclear whether any of the existing legislation will become law, what is clear is that issues relating to privacy and cybersecurity will continue to be a focus of discussion, with continued pressure on Congress to implement federal legislation to harmonize requirements and provide a unified approach to data protection across the United States.

V. Conclusion

The trend toward greater data privacy and protection, both inside and outside the U.S., looks to continue, with increasing numbers of countries adding data privacy protection or expanding existing laws governing data privacy. In the U.S. and elsewhere there is a greater emphasis on providing data subjects with more control of their personal data and greater recourse for the loss or misuse of their data. Even within the U.S., which tends to offer less legal protection for data privacy, we are seeing an uptick in fines, penalties, and litigation for data breaches and misuse of personal data.