Skadden

Privacy & Cybersecurity Update

EU Unveils Sweeping Changes to Its Privacy Laws

The EU has approved a new General Data Protection Regulation. While it will not go into effect until two years after its formal adoption in the coming few months, its broad and sweeping changes will require many companies to start planning their compliance in 2016.

Some four years after the European Commission first proposed enacting a new data protection regime to replace the 1995 EU Data Protection Directive (the 1995 Directive), the European Parliament and Council of the European Union (the Council) have announced a sweeping new EU data protection regulation. The impact of the new General Data Protection Regulation (GDPR, or the Regulation) cannot be overstated. It will impact not only companies established in the EU, but also non-EU companies that process personal data of EU residents.

The GDPR must still be formally adopted by the Council and then approved by the European Parliament, but this is likely to occur in the first quarter of 2016. And, while the intense lobbying by the business community and privacy advocates over the last four years is likely to continue between now and when the GDPR is finally voted into law, we do not expect any material substantive changes to the 200-page draft. Since the GDPR is a regulation and not a directive, it does not require an enabling law to be passed by each member state. Rather, the Regulation will apply to all member states. Nonetheless, there are a number of provisions that permit "customization" by member states such that many companies may still feel they are dealing with multiple data protection laws across Europe.

The GDPR will go into effect two years after it has been published in the Official Journal of the European Union. While this means that the GDPR will not go into effect until mid-2018, the broad and sweeping changes it introduces means that any company that does business with EU residents or has EU employees will likely need to use much of the next two years to plan its future compliance.

The final text of the GDPR highlights that the EU has a very different view of privacy, and particularly the balance between privacy and digital commerce, than many other countries, including the United States. For example, in the U.S., consumers have demonstrated a willingness to trade off use of their personal data for a seamless digital experience and enhanced services. While all consumers have a line beyond which such data usage feels too intrusive, they also do not necessarily want the burden of being asked for consent each and every time their data is used. The GDPR "resolves" this tension by imposing strict explicit consent requirements on almost all uses of data. We will see in the coming years whether this will ultimately hamper digital innovation in the EU or be seen as the new global normal. Those outside the EU must keep in mind that the EU recognizes a "fundamental right" to an individual's "protection of personal data," which drives many provisions of the GDPR. Any company that is balancing its own business interests and those of the data subject should keep that principle in mind.

We provide below a guide to some of the key provisions of the GDPR. This guide is not meant to be exhaustive of all of the topics covered by the GDPR, and even within specific topics, we have not covered all of the nuances. The Skadden Privacy and Cybersecurity team is available to discuss specific aspects of the GDPR in greater detail.

Scope of Coverage

To Whom Does the GDPR Apply?

The GDPR applies more broadly than the 1995 Directive. Like the 1995 Directive, the GDPR applies to data controllers and data processors located in the EU. However, the GDPR also applies to data controllers and data processors located outside the EU if the data processing activities relate to (i) the offering of goods or services to EU data subjects (regardless of whether a payment for the goods or services is required), or (ii) the monitoring of the behavior of EU data subjects to the extent that behavior takes place in the EU. (Article 3) In contrast, the 1995 Directive applies to data controllers (not data processors) located outside the EU only if they process personal data in connection with the activities of an establishment in the EU, or if they use equipment located in the EU to process data. Accordingly, companies will need to evaluate whether their data processing activities that were outside the scope of the 1995 Directive will be subject to the GDPR.

The introductory paragraphs of the GDPR offer some guidance to help companies located outside the EU determine whether they would be considered to fall within the scope of the Regulation. For example, the remarks state that the mere accessibility of the company's website in the EU, or the use of a language generally used in the country where the company is located, is insufficient to deem the company's activities within the scope of the GDPR. If, however, the company uses a language or currency used in a member state, with the possibility of ordering goods in that language, then the company's activities may be deemed within the scope of the GDPR. (Whereas Clause 20) In addition, a company located outside the EU may be said to monitor the behavior of EU data subjects if the company uses data processing techniques to profile an individual to make decisions about an individual or to predict his or her personal preferences. (Whereas Clause 21)

What Personal Data Is Covered?

Under the 1995 Directive, there was some uncertainty as to what information constituted "personal data." The GDPR has eliminated such uncertainty, largely by expanding the definition. Under the GDPR, "personal data" includes any information that can be used to identify an individual "directly or indirectly," including through a name, identification number, location data, and online identifier. This would therefore include e-mail addresses tied to a specific company (*e.g.*, JohnDoe@CompanyX.com) as well as device identifiers where the device can be linked to a specific individual. The definition also includes the use of factors that alone or in combination can be used to identify an individual (such as physical, cultural and economic information).

Pseudonymization

A common question from data controllers and processors is whether "anonymized" data is subject to the same treatment as personal information. The GDPR recognizes that there is a category of data between fully anonymized and personally identifiable. This category of "pseudonymization" is defined as the processing of data such that the individual can no longer be identified without additional information. The data controller or data processor can continue to hold the information that would allow such an individual to be identified, so long as such information is kept separate and is subject to technical and organizational measures that allow the individual to remain nonidentified.

Profiling and Automated Decision-Making

The GDPR introduces the concept of "profiling," which is defined as any automated processing of personal data in order to analyze or predict aspects concerning an individual's "performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." (Article 4) In general, data controllers must inform data subjects when automated decision-making, including profiling, is being used

that has a legal effect, and give the data subject the right to object. (Articles 14(h) and 20) Data subjects can also object to the use of profiling for direct marketing purposes. (Article 19) Given the growing use of data mining and profiling to make decisions about individuals, the GDPR's strict limitations could have a material impact on how companies do business with European residents.

Lead Data Protection Authority

The supervisory authorities having jurisdiction over a data controller or a data processer are divided into two types: a lead supervisory authority and "concerned" supervisory authorities. In theory the lead supervisory authority is to act as a "one-stop shop" so that data controllers and data processors are not required to interact with a number of different supervisory authorities, as they do under the 1995 Directive. In practice, however, a controller or processor could still be required to interact with multiple authorities (*e.g.*, in cases where complaints are lodged by data subjects with multiple supervisory authorities).

The lead supervisory authority is the one in which the main establishment of the data controller or data processor in the EU is located. (Article 51a) A data controller's main establishment in the EU is its place of central administration, unless the management decisions on processing of personal data are made in another place in the ordinary course, in which case such place is its main establishment. (Whereas Clause 27, Article 4(13)) A data processor's main establishment in the EU is its place of central administration or, if there is no place of central administration, the place where the main processing activities that are subject to the GDPR occur. (Article 4(13))

A concerned supervisory authority is one (i) in which the data controller or data processor is established, (ii) in which data subjects that are substantially affected by the processing reside, or (iii) that has received a complaint about personal data processing. (Article 19(a))

The lead supervisory authority is the sole contact for the controller or processor for all cross-border processing matters. It also coordinates with concerned supervisory authorities to address all data processing matters (whether cross-border or not). In some cases, the lead supervisory authority can decide to allow the concerned supervisory authority to handle an issue directly with the data controller or data processor. (Article 51a) All supervisory authorities cooperate and exchange information with the goal of reaching consensus regarding the handling of data processing matters for data controllers and data processors within their respective jurisdictions. (Article 54a) If, despite such cooperation, the lead supervisory authority and a concerned supervisory authority disagree on a decision, the matter is referred to the European Data Protection Board for a binding decision. (Article 58(a))

Processing Activities

Fundamental Principles

The GDPR requires that the data controller[1] be able to demonstrate that any personal data it controls is:

- processed fairly and in a transparent manner;
- collected for "specified, explicit and legitimate purposes" and not processed in a way incompatible with those purposes;
- limited to what is necessary for the processing;
- accurate (and promptly corrected or erased if it is not accurate);
- kept in a nonanonymized form only for so long as necessary to conduct the processing; and
- protected from unauthorized access using "appropriate technical or organizational measures."

The transparency requirement is somewhat more rigorous than was required under the 1995 Directive. For example, the data controller must inform the data subjects of the legal basis upon which it is relying to process data. This requirement will likely yield more robust privacy notices, but it remains to be seen whether they are any clearer to data subjects.

Obligations to Obtain Consent

One of the most hotly debated privacy issues today is the extent to which an organization must obtain explicit consent from the data subject before engaging in processing that is beyond what is required to fulfill a contract with a customer. Companies would, of course, prefer the right to obtain broad consent through an opt-out mechanism. Examples include provisions of online privacy policies that state that by using a service, the data subject consents to having their data shared with third parties, and online forms in which a user must explicitly check a box in order" not to receive promotional offers. The GDPR eliminates such mechanisms by defining consent as a "freely given, specific, informed and unambiguous indication of [the data subject's] wishes." This can be through a statement or "by a clear affirmative action." (Article 4) The whereas clauses clarify that "silence, pre-ticked boxes or inactivity" do not constitute consent. (Whereas Clause 25) The GDPR also strongly suggests that consent is required for each new processing activity. Thus, while a company can rely on a single consent to provide a series of promotional materials to a consumer, it likely could not rely on a broad consent to provide the user's data to multiple, unnamed third parties for unspecific general marketing purposes.

[1] A data controller is the individual or entity that can determine the purpose and means of how personal data is processed.

Data controllers also cannot rely on broad language that covers a myriad of topics including data processing consent. Instead the request for data processing consent must be presented "in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language." (Article 7)

The data subject must be informed they have the right to withdraw their consent at any time, and must be able to do so as easily as the process used to obtain their consent. Once consent is withdrawn, the data subject's personal data can no longer be used, but it does not impact any processing that took place before the withdrawal. (Article 7)

Processing of Children's Data

The EU has recognized that special protections need to be implemented with respect to the collection of personal data from children since they may be "less aware of risks, consequences, safeguards and their rights." (Whereas Clause 29) The GDPR applies an approach similar to the U.S. Children's Online Privacy Protection Act (COPPA) by requiring that parents' provide consent, or authorize consent for anyone under the age of 16. (Article 8) Since member states have the right to lower this age to 13, the controller must make reasonable efforts to verify that a parent actually provided such consent "taking into consideration available technology."

Data Protection and Privacy by Design

The GDPR requires data controllers to implement data protection policies "proportionate in relation to the processing activities" and that take into account the cost of implementation. (Articles 22 and 23) While the GDPR does not specify those policies, the fact that the Regulation recognizes that there is no single solution, and that the policy can be proportional to the processing undertaken, will be welcome by most companies. The GDPR also states that protective measures should be implemented when the processing is designed in order to meet the data protection requirements. This includes setting, as a default, that only the minimum amount of data necessary for a purpose is processed. (Article 23) The need to implement privacy protections in the design of services is a step that companies should begin taking during the two-year pre-implementation period.

Designation of a Data Protection Officer

Data controllers are required to designate a data protection officer in certain cases, including where:

- the data controller or data processor is not located in the EU but engages in the data processing activities that make it subject to the GDPR (summarized above) (Article 25);
- the core activities of the data controller require systematic monitoring of data subjects on a large scale (Article 35); or
- the core activities of the data controller consist of large-scale processing of certain sensitive categories of data, such as racial or ethnic origin, political opinions, genetic information, sexual orientation and criminal offenses.

The data protection officer must have expert knowledge of data protection law and practices. The officer can be either an employee or a contractor but in either case must report directly to the highest management level of the controller. (Article 36) The officer's duties include advising the data controller of its obligations under the GDPR and serving as the main contact for data subjects and the supervisory authorities. (Article 37)

Impact Assessment and Prior Consultation

Unlike the 1995 Directive, which includes a general obligation to notify the supervisory authority of the processing of personal data without regard to the level of risk posed by the processing, the GDPR requires such notification only where the processing poses a high risk to the data subjects. (Article 33) The supervisory authorities are charged with creating a specific list of such situations, but the introductory clauses of the GDPR suggest that impact assessments are likely to be required in cases where the processing takes place on a large scale using new technology, where the personal data is used for profiling purposes and where the processing activity involves monitoring public places on a large scale (*e.g.*, using facial recognition technology). (Whereas Clause 71) The impact assessment should describe the data processing performed by the data controller, the proportionality of the processing in relation to its purpose, the risks to the data subjects and the ways the data controller plans to mitigate such risks. (Article 33)

If the impact assessment shows that the data processing poses a high risk, the data controller must consult with the supervisory authority prior to undertaking the processing. If the supervisory authority determines that proposed activities would not comply with the GDPR (*e.g.*, if the data controller's proposed measures to mitigate the risk are inadequate), the supervisory authority will advise the data controller regarding the risks and appropriate mitigation. (Article 34)

Transborder Data Flow

The limited ability of companies to send personal data about EU residents outside the EU was a foundation principle of the 1995 Directive, and it remains so in the GDPR. The new Regulation retains the same basic structure as the 1995 Directive; namely, that unless a country ensures an "adequate" level of protection, data transfers to that country are prohibited unless an acceptable alternative is in place. (Article 41) Those countries that were

already approved, such as Canada and Israel, remain approved. Transfers to other countries, such as the United States, will require use of binding corporate rules (which we anticipate will continue to be rarely used); data protection clauses (such as the "model contracts" that are used today); or an approved code of conduct that has binding and enforceable commitments. (Articles 40-45) In addition, the data protection authorities of member states will be able to issue standard contract clauses on which organizations may rely.

Exclusions for Small- and Medium-Sized Companies

The GDPR contains some exclusions for organizations with fewer than 250 employees that only engage in periodic processing of nonsensitive data. Such organizations are not required, for example, to maintain detailed records of the data they are processing and their processing activities and do not have to name a data protection officer. (Article 28)

Data Subject Rights

Right of Access

The GDPR continues the 1995 Directive's requirement that data subjects have access to the personal data that a controller holds about them. Such information must be provided "without undue delay" and within one month of the request (with a right to extend the period to two months if the request is complex or voluminous). (Article 11) The information the data subject can obtain includes, among other areas: the identity of the data controller; the purpose of the processing; the recipients of the data; how long the data will be stored for; and the extent to which any automated data processing is being performed. (Article 14) This information must also generally be provided even where the controller did not receive the data directly from the data subject. (Article 14a)

The Right to Be Forgotten

The GDPR codifies the so-called "right to be forgotten," which provides for a right for data subjects to request that data controllers erase personal data about them. A 2014 Court of Justice of the European Union case[2] had established that such a right existed under the 1995 Directive, but the GDPR is the first EU effort to define the parameters of this right in a statute. The GDPR also identifies a number of exceptions to this right that could, theoretically, significantly limit its scope.

General principle. The GDPR states (in Article 17) that the data subject has a "right to obtain from the data controller the erasure of personal data concerning him or her without undue delay" and that data controllers must comply with that request where at least one of the following applies:

- the data is no longer necessary for the purpose for which it was collected or otherwise processed;
- the data subject withdraws the consent on which the processing was based, and there is no other legal ground for the data processing;
- with respect to certain types of data processing, the data subject objects to the processing;
- the data has been unlawfully processed;
- the data has to be erased in order to comply with an EU or EU member state law that applies to the controller; or
- the data was collected as part of an information society service directed to children.

Although there are some exceptions to these requirements (which we discuss below), there is no exception for archival copies of personal data, or from data held by its data processors. Based on the plain language of the GDPR, companies that receive erasure requests from data subjects must erase the data from all media in their control, and would have an obligation to ensure that their processors do so as well, which in many cases could be a complex and significant undertaking.

Erasure following public disclosure. In a provision that seems targeted at publishers, website operators and search engines, if a controller is required to erase personal data that it has made public, it must take reasonable steps to inform other controllers that are processing the data that the data subject has requested its erasure. However, the scope of this obligation may take into account available technology and the cost of implementation. Nevertheless, it is clear that the European Commission seeks to provide data subjects with some tools to have information removed from public view. (Article 19)

Important limitations on right to be forgotten. The GDPR includes a number of limitations on the Regulation's requirements. For example, data erasure is not required where the data processing is "necessary" for exercising the right of freedom of expression and information, or for the establishment, exercise or defense of legal claims.[3] It is not yet clear how EU data protection

[2] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, Case C-131/12, 13 May 2014, available at http://curia.europa.eu/juris/documents.jsf?num=C-131/12. We discussed this case in our May 2014 edition of the Privacy & Cybersecurity Update, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_May_2014.pdf.

[3] Other exceptions in Article 19(3) include processing that is necessary for (i) compliance with an EU or EU member state legal obligation, (ii) performance of a task carried out in the public interest, (iii) the exercise of official authority vested in the data controller, (iv) reasons of public interest in the area of public health, and (v) archiving purposes in the public interest or scientific and historical research purposes or statistical purposes, if erasing the information would seriously impair the objectives of the archiving purposes.

authorities and courts will interpret these exceptions. Does the Regulation permit a social media service to refuse to remove information reposted by its users on the ground that doing so would be inconsistent with the free flow of information? Does the right to refuse a request to erase information based on the need to establish or defend a legal claim justify a company maintaining customer or employee information for so long as a claim could be brought, even if none is threatened? When is processing of personal data truly "necessary" for exercising the rights of freedom of expression and information? Until these and other similar questions are answered, the scope of the right to be forgotten will likely be widely debated and contested.

Right to Restriction of Processing

Similar to the "right to be forgotten," a data subject has the right to restrict the processing of his or her personal data, though in far more limited circumstances. (Article 17) Specifically, data subjects have a right to require a data controller to restrict the processing of personal data in certain circumstances, including where:

- the accuracy of the data is contested by the data subject (but the restriction period only lasts for so long as it takes the data controller to verify the accuracy of the data);
- the data processing is unlawful, but the data subject objects to the erasure of the data and requests restriction of its use instead; or
- the data controller no longer needs the data for the purpose of the processing, but the data subject requires the controller to retain it for the establishment, exercise or defense of legal claims.[4]

Once a data subject has requested restricted processing, the personal data may only be processed (i) for storage, (ii) with the data subject's consent, (iii) for the establishment, exercise or defense of legal claims, (iv) to protect the rights of another person, or (v) for reasons of important public interest of the EU or a member state.

Right to Data Portability

The GDPR gives data subjects a right to receive a copy of the data he or she has provided to a data controller and to provide that data to another data controller, under certain circumstances. (Article 18) Such data must be provided in a "structured and commonly-used and machine readable format," which could be problematic for companies that use proprietary database architectures. This right only applies where the data controller uses automated data processing, and the processing is either done (i) with the data subject's consent, or (ii) in order to perform a contract with the data subject.

[4] Article 17(a)(1) also includes a right to require restrictions on the processing of personal data where the processing is not done with consent but rather because it is necessary for (i) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or (ii) the purposes of the legitimate interests pursued by the controller or by a third party.

Data Security and Data Breach Notification

Data Security Requirements

The GDPR requires data controllers and data processors to use appropriate measures to ensure a level of security of personal data that is appropriate to the risks presented by the processing of such data. (Article 30) These measures may include:

- pseudonymization and encryption of personal data;
- the ability to ensure the confidentiality and availability of systems that process the data;
- the ability to restore access to such systems in a timely manner in the event of an incident; and
- a process for regular testing of the effectiveness of these security measures.

In assessing what measures may be appropriate, companies should consider industry standards, the cost of implementing the measures and the purpose of the processing, including the risks arising from unauthorized access to the personal data. A company's compliance with an approved code of conduct or an approved certification mechanism may be used to help demonstrate that the company's security measures are appropriate to the risk, but is not necessarily conclusive by itself. (Article 30)

Data Breach Notice Requirements

Notice to the supervisory authority. In the event of a personal data breach, the GDPR requires the data controller to notify the competent supervisory authority without undue delay and, where feasible, within 72 hours after discovery of the breach (unless the breach is unlikely to result in any risk to the data subject in which case no notice is required). If the notification is made more than 72 hours after discovery, the notice must be accompanied by an explanation for the delay. (Article 31) The notice to the supervisory authority must at a minimum:

- describe the nature of the breach, including the categories and number of data subjects involved;
- give the contact information for the data controller's data protection officer;
- describe the likely consequences of the breach; and
- describe the measures to be taken by the data controller to address the breach.

If all of the foregoing information cannot be provided at the same time, the information may be provided in phases, but in any event without undue delay. (Article 31) In practice, all of the facts of a data breach are not typically known within 72 hours; it can take days or even months for companies (often with the assistance of an outside technical consultant) to ascertain the

number and type of records affected. Accordingly, under the GDPR, companies may find themselves having to make multiple notices to the supervisory authority as more facts come to light over the course of the investigation.

For U.S. companies that are subject to the GDPR, the 72-hour notice requirement will seem stringent in comparison to those under state data protection laws, which typically require notice of the breach to be sent to the applicable state authority but which often include a threshold to be met before notice is required (*e.g.*, 1,000 data subjects affected) and either do not specify a time in which such notice must be provided or specify a much longer period of time (*e.g.*, 45 days) which is tied to when notice to data subjects is provided.

Notice to the data subjects. In the event of a personal data breach, in addition to notice to the supervisory authority, in certain cases the data controller must also send a similar notice to the data subjects affected if the breach is likely to result in a high risk to the rights of the data subject. (Article 32) Interestingly, this "high risk" trigger is a higher bar than the trigger for the notice to the supervisory authority, and there is no timeframe specified for the notice to the data subjects other than "without undue delay." In addition, despite the GDPR's overall emphasis on the rights of individuals, the notice to data subjects is not required if the data was encrypted, if the controller has taken measures to ensure that the high risk is not likely to materialize, or if giving the notice would involve "disproportionate effort," in which case a public communication is sufficient (although the supervisory authority can require notice if it believes one is required). The introductory clauses of the GDPR emphasize that the notice to data subjects should be made in close cooperation with the supervisory authority and other law enforcement so that, for example, a criminal investigation is not jeopardized by an early disclosure of the breach.

Liability and Penalties

Joint Liability for Controllers and Processors

In a move that is certain to heighten data controller oversight over their data processors, and increase the focus on liability provisions in their contracts, the GDPR provides that data controllers and processors are equally liable to pay compensation to data subjects for violations of the Regulation (Article 77). The article also provides that if the controller or processor pays full compensation to the data subject for the damage suffered, it is entitled to seek a proportional share of the damages from the other party, based on their respective responsibilities for the violation.

Penalties for Violating the GDPR

Perhaps the most controversial aspect of the GDPR is the imposition of large penalties for violations of its provisions. Intense lobbying by the business sector resulted in some changes from the initial proposal, but the penalty provisions in the final proposal remain very stringent.

When penalties are imposed. In general, the GDPR permits each member state's supervisory authorities to impose administrative fines in addition to, or instead of, issuing warnings or imposing procedural requirements or limitations on data controllers and processors. These fines are to be "effective, proportionate and dissuasive." When deciding whether to impose an administrative fine and deciding on the amount, the GDPR requires that the supervisory authorities take into account a number of factors, including (Article 78(2a)):

- the nature, gravity and duration of the violation (and whether the violation was intentional or negligent);
- actions taken by the data controller to mitigate the damage suffered by the data subject;
- the degree of responsibility of the controller or processor, taking into account technical and organizational measures implemented by them;
- the type of personal data affected by the violation;
- how the violation became known to the supervisory authority, especially whether the controller or processor reported the violation itself; and
- any other aggravating or mitigating factors.

These criteria will directly impact how companies operate, including whether they "self-report" violations they discover and how data controllers manage and control their data processors.

Penalty amounts. If a supervisory authority decides to levy an administrative fine against a data controller or processor, the size of the fine is subject to certain limitations based on the part of the Regulation that has been violated. The maximum penalties for violating the Regulation vary based on the type of violation. In general, the maximums are based on the greater of a specified amount and, for companies, a percentage of their revenues. (Article 78)

For certain violations, the maximum fine is the greater of €10 million and, for companies, 2 percent of total worldwide revenues of the preceding fiscal year. (Article 78(3)) The GDPR identifies 19 different articles that, if violated, are subject to these caps, including articles on topics such as:

- obtaining parental consents for processing information related to children;
- a controller's obligation to implement organizational and technical measures to protect privacy;
- obligations relating to the use of data processors;
- data breach notification obligations;

- obligations regarding conducting data assessments before engaging in a new type of data processing; and
- obligations regarding the appointment and responsibilities of data protection officers.

For other violations, Article 78 establishes maximum fines of the greater of €20 million and 4 percent of total worldwide revenues of the preceding fiscal year. (Article 78(3a and 3aa)) These caps apply to over 20 different articles or other provisions in the GDPR, including:

- the fundamental data processing principles;
- the requirements for obtaining consent from data subjects;
- data subjects' rights regarding access to information, the right to be forgotten, the right to restrict the use of data, data portability obligations and the right to object to automated data decision-making;
- obligations relating to the transfer of personal data to third countries; and
- noncompliance with an order of a supervisory authority;

Companies of all sizes have objected to the foregoing penalty structure. Large companies have argued that they face larger penalties simply because of their size, even if such size has no relation to the extent of their data processing activities. Smaller companies have objected that a €10 million or €20 million fine could effectively drive them out of business. The GDPR's admonition that the fines be "effective, proportionate and dissuasive" (with no express limitations based on the impact on the company being fined) suggests that data protection authorities may use fines for their maximum deterrent value, depending on the circumstances.

Return to Table of Contents

Cybersecurity Information Sharing Legislation Passed Into Law

The Cybersecurity Act of 2015, recently signed into the law by President Barack Obama, provides new authorities for private-sector entities to monitor for threats and share cybersecurity threat information and defensive techniques. While the new law closes more than a decade of debate over an appropriate federal response to cybersecurity, it remains to be determined whether the private sector's use of information sharing techniques has been constrained by legal concerns or by other considerations.

The omnibus appropriations legislation signed into law by President Obama on December 18, 2015 (Consolidated Appropriations Act, 2016) included the Cybersecurity Act of 2015 (the Cybersecurity Act). The Cybersecurity Act will alter the rules governing the sharing of cybersecurity information within the private sector and between the private sector and the government. While the passage of the Cybersecurity Act ends more than a decade of negotiations in Congress regarding the ultimate shape of cybersecurity information sharing legislation, it begins the debate over how the new information sharing rules should and will alter private-sector behavior.

Title I of the Cybersecurity Act, also known as the Cybersecurity Information Sharing Act of 2015, or CISA, creates a number of new authorities permitting private-sector entities to monitor and share information. Collectively, those authorities are intended to enhance federal government information sharing with the private sector and to encourage private-sector entities to monitor for cybersecurity threats, share cybersecurity threat information voluntarily with the federal government and share such information with each other.

Where CISA adds new sharing authorities, it primarily addresses the sharing of "cyber threat indicators" and "defensive measures." The former includes information that is "necessary to describe or identify" any one of a number of different activities or situations that may indicate the presence of cybersecurity vulnerabilities, such as malicious reconnaissance or the harm caused by exfiltration of data. The latter includes an action or other measure applied to information systems that "detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability" without harming that information system.

Private-sector entities are authorized under CISA to:

- monitor their own information systems and those of consenting third parties for "cybersecurity purposes" (*i.e.*, "protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability");
- operate defensive measures on their own information systems and those of consenting third parties in order to protect the owner's rights and property; and
- share cyberthreat indicators and defensive measures with other entities — both those in the private sector and those in federal government — for a cybersecurity purpose.

The law establishes these authorities "notwithstanding any other provision of law"; this language is intended to give private-sector entities the power to monitor traffic and share information despite the limitations in pre-existing surveillance laws. CISA

also includes an explicit antitrust exemption allowing entities in the same industry to collaborate by sharing cyberthreat indicators or defensive measures or providing "assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes."

In addition, CISA creates incentives for private-sector information sharing by limiting the government's ability to use such information and the entities' liability for sharing it. The law specifies that sharing does not waive privileges or legal protections and does not subject the shared information to disclosure under the Freedom of Information Act. It states that information may be shared within the executive branch only for cybersecurity purposes, or for certain specific law enforcement and national security purposes, and that shared information may not be used in enforcement or regulatory actions against the sharing entity. It states that "no cause of action shall lie" against any private-sector entity monitoring traffic pursuant to the law. In addition, it limits private-sector entity liability for sharing cyberthreat indicators or defensive measures, as long as (i) the entity shares information pursuant to the terms of the law, including provisions protecting against sharing of personal and private information, and (ii) information shared with the government is provided solely to the Department of Homeland Security (DHS) through the process to be established pursuant to the law.

Finally, the new law also encourages sharing of information from the government to the private sector. CISA requires the government to develop and issue procedures to promote timely sharing of both classified and unclassified cyberthreat indicator information and defensive measures with the private sector. The Cybersecurity Act generally also calls for the government to develop real-time information sharing capabilities, and encourages the use of existing entities, such as sector-specific information sharing and analysis centers (ISACs).

Takeaways

While the Cybersecurity Act contains a number of other provisions addressing everything from federal cybersecurity workforce preparedness to reporting on mobile device cybersecurity issues, information sharing has been developed as the centerpiece of the new law. However, while the authors have indicated that they expect CISA to encourage private-sector entities to share more information with the government, it is not yet clear how widely adopted this new cybersecurity information sharing model is likely to be.

Many private-sector entities already share cyberthreat information with other private-sector actors, whether through independent third parties such as the ISACs or through cloud-based cybersecurity toolsets provided by cybersecurity solution providers. The added incentive of limitations on liability may encourage legally cautious private-sector entities to begin sharing information with peers or even the government, but it remains possible that the greatest barriers to information sharing will continue to be costs and reputational risks rather than legal limitations.

In addition, in a few industries, private-sector entities already have close relationships with regulators or other government agencies responsible for maintaining the security of private-sector companies within specific sectors of the economy. Those private-sector entities may have little or no pre-existing relationship with DHS, and the agency may need to engage in significant outreach before the private sector is prepared to accept it as a trusted partner.

Return to Table of Contents

Wyndham Settlement With FTC Provides Insights

The long-running and precedent-setting dispute between Wyndham Hotel and Resorts LLC (Wyndham) — a subsidiary of Wyndham Worldwide Corporation — and the Federal Trade Commission (FTC) regarding Wyndham's allegedly lax data security practices finally came to a close on December 9, 2015, when the two parties filed a stipulated settlement agreement in the U.S. District Court for the District of New Jersey.

Background

The FTC/Wyndham action began in 2012 when the FTC issued a complaint against the company related to three separate data breach incidents that occurred between 2008 and 2009. Rather than settle with the FTC, as 50 companies had previously done when faced with similar complaints, Wyndham moved to dismiss the claim in federal court. Its motion was premised on three primary arguments: (i) the unfairness standard under the FTC Act did not encompass unreasonable data security measures, (ii) the FTC had not given businesses like Wyndham due notice that unreasonable data security measures were unfair under the FTC Act, and (iii) the FTC's complaint did not sufficiently allege consumer injury as required by the FTC Act. The New Jersey District Court rejected all of these arguments and denied Wyndham's motion to dismiss the complaint.

Wyndham filed an interlocutory appeal with the U.S. Court of Appeals for the Third Circuit. In August 2015, in a unanimous opinion, the Third Circuit upheld the District Court's ruling that the FTC had the authority under the FTC Act to bring lawsuits against companies for their inadequate and ineffective security

practices. Particularly noteworthy about the Third Circuit's holding was the sentiment expressed by the court that companies like Wyndham are on notice about what the FTC considers "unfair" with respect to data security practices because there is a history of FTC settlements and consent decrees on the topic.

The Settlement

Although the settlement shares many characteristics with other settlements the FTC has reached with companies with respect to credit card and data security practices, the Wyndham settlement has some important differences — particularly regarding the franchisee/franchisor relationship — that help shed light on what the FTC expects from other companies going forward. The settlement requires Wyndham to establish a comprehensive information security program designed to protect the payment card information of its customers. However, the settlement provides that Wyndham will be deemed in compliance with its obligations under this aspect of the agreement if it passes an annual audit finding it to be in compliance with the Payment Card Industry Data Security Standard (PCI DSS). This suggests that the FTC may deem compliance with PCI DSS as a "reasonable" standard for companies to follow in order to comply with their data security obligations as it relates to credit card data.

Second, the settlement requires that if Wyndham experiences a future data breach affecting more than 10,000 payment card numbers, it must obtain an assessment of the breach and provide that information to the FTC within 10 days. While 10 days is not particularly long, many suspected that the FTC would have demanded an even shorter notice period.

Third, Wyndham is required to establish effective barriers, such as firewalls, between its corporate servers and databases and those of its franchisees, in order to reduce the risk of a repeat attack. According to the FTC, the three data breach incidents involved hackers' obtaining access to a Wyndham franchisee's network, and then exploiting weaknesses in the architecture of the Wyndham corporate network to gain access not only to the corporate servers, but also dozens of other franchisees' databases. In order to prevent this type of incident going forward, Wyndham will be required to ensure that its corporate networks are adequately separated from and secured against its franchisees' networks. However, the settlement imposes no obligations on Wyndham to ensure that its franchisees' networks are secure in their own right or to oversee their data security practices.

While this latter aspect of the agreement obviously provides useful insight with respect to how the FTC views the franchisor/franchisee relationship, it may also provide some guidance on how companies should organize their relationships with other third parties outside their networks. If the FTC believes that a franchisor should takes steps to protect its network from its franchisees, it is reasonable to assume that at least those same steps should be taken to protect a corporate network from the networks of third-party vendors and other entities with which companies may share data.

Conclusion

The settlement agreement between Wyndham and the FTC marks the end of a significant challenge to the FTC's authority under the FTC Act to regulate and punish companies for allegedly lax data security practices. Following the Third Circuit's ruling, the current legal landscape supports the proposition that the FTC does, in fact, have the authority to go after companies for failing to adequately secure their customers' personal data, particularly payment card data. However, as the Third Circuit noted in its opinion, by examining FTC settlement agreements addressing data security, including the agreement with Wyndham, companies can adopt practices that the FTC is likely to find reasonable, and thereby minimize the risk of FTC prosecution following a data security incident.

Return to Table of Contents

CFTC Proposes Cybersecurity Regulations

The CFTC became in December the first regulator to propose cybersecurity regulations. The regulations, which may signal an increased interest by regulators in issuing actual regulations, would require CFTC-regulated organizations to administer five types of cybersecurity testing, some on a regular schedule.

On December 16, 2015, the U.S. Commodity Futures Trading Commission (CFTC) unanimously approved new cybersecurity regulations for critical infrastructures the CFTC regulates (such as electronic trading platforms, clearing organizations and data repositories). The proposed regulations will be open for public comment during a 60-day comment period after the regulations are published in the Federal Register. While other financial service regulators have issued guidance and suggested monitoring tools in the area of cybersecurity, the CFTC is the first regulator to propose actual regulations, and may be a harbinger of similar steps by other regulators.

The regulation would introduce five types of testing, specifying the frequency with which some tests must be administered, and requiring that the board review the test results. Organizations

that fail a test would have to establish a remediation plan to cure the applicable deficiency. The five test areas are as follows:

- **Vulnerability Testing.** While most organizations already scan their systems for system vulnerability, the new regulation would make this a formal requirement, and large organizations would have to conduct such testing on a quarterly basis. Two of such tests each year would have to be conducted by an independent contractor.
- **Penetration Testing.** Almost all guidance today lists penetrations testing as a best practice to identify security risks. However, as with vulnerability testing, this would now be a formal regulation, with requirements to test for the risk of internal and external attacks.
- **Controls Testing.** In addition to testing for vulnerabilities, organizations will now be required to test, over a two-year rolling period, the key controls in their cybersecurity program, with large organizations required to conduct this testing using an independent contractor. Such testing "includes testing of all [of an organization's] system safeguards-related controls," such as which users have access to which data and systems.
- **Security Incident Response Plan Testing.** Implementing and testing security incident response plans (SIRPs) is a standard component of most organizations' cybersecurity programs, and therefore this regulation should not impose any additional burden on CFTC-regulated entities.
- **Enterprise Technology Risk Assessment.** Under the new regulations, organizations are required to conduct an annual assessment of the cybersecurity risks they face and the damage that would be caused by such incidents. Risk assessment should already be a standard component of an organization's cybersecurity planning, but the requirement that this be done annually may require more frequent assessments. However, such risk assessments are valuable, and most organizations will benefit from this annual review.

If you would like assistance crafting a comment to the proposed regulation, please contact a member of the Skadden Privacy and Cybersecurity team.

Return to Table of Contents

(Attorney contacts appear on the next page.)

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James R. Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Ivan A. Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David E. Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jennifer L. Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Helena J. Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Gregoire Bertrou
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com