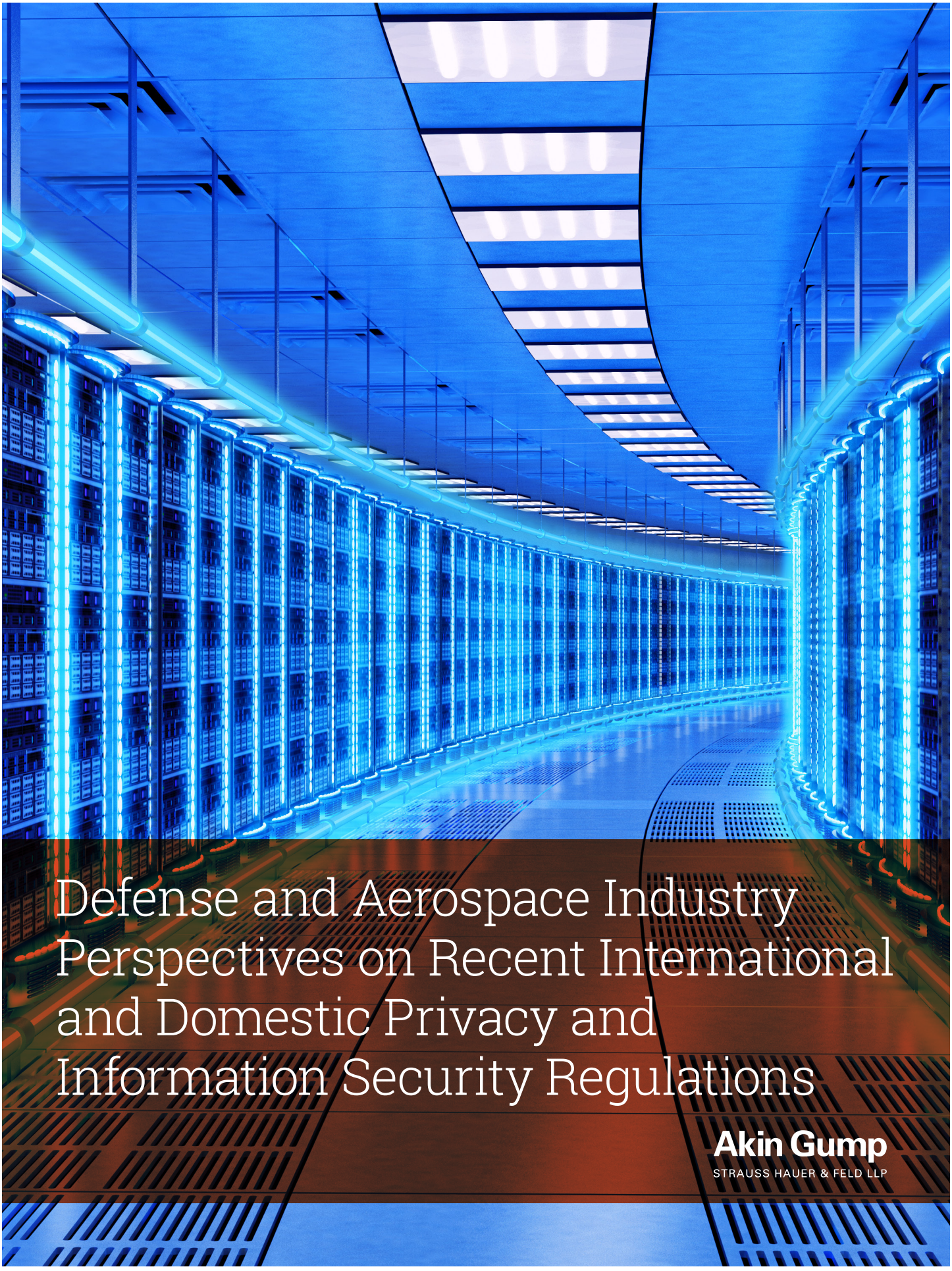

Defense and Aerospace Industry Perspectives on Recent International and Domestic Privacy and Information Security Regulations

Akin Gump
STRAUSS HAUER & FELD LLP

Companies in the defense and aerospace industries are facing increasing obligations with regard to overlapping national and transnational data protection and information security regimes. These overlapping and complex regimes may, on first glance, appear to differ significantly from one another, yet a closer read shows that they often include similar obligations. Developing a high-level approach to compliance can help companies meet cross-regime minimum requirements efficiently, reserving time and energy for more complicated regime-specific requirements.

This White Paper seeks to provide defense and aerospace companies with a blueprint for tackling cross-regime compliance by providing a working set of proactive measures to implement now. These measures are not intended to ensure full compliance; rather, they offer a jumping-off point for comparing the various regulatory regimes in play and identifying key points of overlap. To facilitate this process, this White Paper examines key provisions applicable to the defense and aerospace industries in the European Union's (EU) General Data Protection Regulation (GDPR), the EU directive on security of network and information systems (the "NIS Directive" or "Directive"), the Asia-Pacific Economic Cooperation (APEC) Cybersecurity Framework (the "APEC Framework"), and the new California Consumer Privacy Act (CCPA) and related California statutes. Using the EU, APEC and California regimes as points of comparison, this White Paper highlights key requirements that are increasingly becoming expected measures.

As we recently discussed in a **prior white paper**, 2018 has already witnessed a number of related developments for defense and aerospace companies in terms of changes to the U.S. Department of Defense's (DoD) acquisition-related guidance and updates to the National Institute of Standards and Technology (NIST) guidelines.[1] Similar developments and related, increasing compliance burdens appear only set to continue.

To help address these expanding compliance burdens, there are a number of proactive measures that defense and aerospace companies can take now to facilitate cross-regime compliance. The most important of these include (1) understanding what you have, where you have it and why you have it; (2) implementing an appropriate, industry-recognized information security framework to ensure adoption of reasonable or appropriate security measures; (3) drafting strong contracts to limit liability for vendor and subcontractor vulnerabilities; (4) crafting processes for tracking protected information and responding to requests related to the same; and (5) bolstering internal governance and oversight of privacy and information security measures. A more comprehensive discussion of these and other proactive measures in provided in Section 2.

1 Akin Gump, White Paper – Recent Department of Defense Guidance on Cybersecurity Requirements and Related Export Control Issues, available at https://www.akingump.com/images/content/8/0/v2/80337/cybersecurity-white-paper-053118.pdf.

Comparing the GDPR, the NIS Directive, the APEC Framework and the CCPA

The GDPR, the NIS Directive, the APEC Framework and the CCPA are each, in their own way, groundbreaking measures. The GDPR, which went into effect on May 25, 2018, enshrines a complex set of rules that are designed to protect data subjects' fundamental privacy rights and update existing privacy laws to reflect and keep pace with new technologies and legal developments, as well as impose a unified and consistent data protection and privacy regime across all EU Member States.[2] The NIS Directive is a first-of-its-kind directive laying out information security principles and objectives that each EU Member State is expected to transpose into its national laws as it sees fit.[3] Its focus is on security, not privacy. The APEC Framework is a set of principles and implementation guidelines that were created in order to establish effective privacy protections aimed at reducing barriers to information flow, and ensuring continued trade and economic growth among the 27 members of APEC. Finally, the CCPA, the newest statute of the group, is focused wholly on privacy concerns and is intended to give California residents greater insight into what information companies collect about them, where that information is collected from, and whether and why the information is sold or shared.

Unlike both the GDPR and the CCPA, the NIS Directive and the APEC Framework rely on member countries' willingness to transpose their general principles into respective national laws. The Directive had a clear deadline of May 9, 2018, for this transposition, while the APEC Framework leaves the timing up to members. To date, only eight or so Member States have fully transposed the Directive, while a handful of others have done so in a partial manner. On July 19, the European Commission sent warnings to the 17 Member States that failed to transpose any portion of the Directive, giving them two months to respond or face further proceedings.[4]

The GDPR and the CCPA, in contrast, have set enforcement deadlines – May 25, 2018, for the GDPR and January 1, 2020, for the CCPA. On those dates, the two statutes either became, or will become, fully enforceable without further action required by regulated territories.[5]

In the following subsections, we compare key elements of these four statutes. The GDPR, the APEC Framework and the CCPA overlap most consistently, since all three deal with privacy and data protection. The NIS Directive is focused on information security and overlaps with the other three statutes only with regard to certain security issues. The points of overlap between any of these statutes are issues of particular importance since those are areas that businesses can target to further efficient cross-regime enforcement efforts.

Scope

Under any of these regimes, defense and aerospace companies may be subject to regulatory requirements, either due to their own status as entities processing data from the respective jurisdictions or as a result of a subsidiary's status as a covered entity.

GDPR: The GDPR divides organizations involved in processing personal data into two categories: (1) data controllers—any person or entity that determines the purposes and means of the processing of personal data, and (2) data processors—any person or entity that processes personal data on behalf of a controller. Defense and aerospace companies are generally controllers, and their subcontractors are usually processors.

2 The GDPR is a mandatory measure that must be adopted by all EU Member States in a consistent manner. In addition to EU Member States, various countries in the European Economic Area (EEA) have also adopted pieces of the GDPR and implemented the same through their national laws.

3 To date, approximately eight European countries have transposed the NIS Directive into their national laws. Other countries are in the process of doing so.

4 The countries targeted by the July 19 warnings were Austria, Bulgaria, Belgium, Croatia, Denmark, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania and Spain.

5 Efforts are under way to amend various provisions of the CCPA. One proposed revision would delay enforcement of the CCPA to the earlier of July 1, 2020, or six months from the date that the California Attorney General's Office publishes its final CCPA-related regulations. Thus, although the CCPA as a whole will go into force on January 1, 2020, it may not be enforceable for another six months.

The GDPR applies to only controllers or processors that (1) maintain an establishment in the EU, if they process personal data in the context of that establishment; (2) are not established in the EU, but offer goods or services to data subjects in the EU; or (3) are not established in the EU, but process the personal data of data subjects in the EU and that data is related to monitoring the behavior of data subjects that occurs in the EU. These categories effectively expand the jurisdiction of data protection authorities beyond the territorial limits of the EU. It is likely that defense and aerospace companies would likely fall within Category 1 or 3.

APEC: The APEC Framework applies to both individuals and organizations in the public and private sectors who **control** the collection, holding, processing, use, transfer or disclosure of personal information ("personal information controllers" or PIC). Individuals are not considered PICs if they collect, hold, process or use personal information for only personal, family or household affairs. The APEC Framework also applies to individuals or entities that instruct others to engage in any of the aforementioned processing activities. In this way, the APEC Framework directly applies to only PICs. It does not apply to entities that might be considered data processors under the GDPR.

CCPA: The CCPA applies to companies that (1) do business in California;[6] (2) collect personal information or, on the behalf of which, personal information is collected; and (3) satisfy one of the following three thresholds: (A) have annual gross revenue of more than $25 million (this is global, not California-specific, revenue); (B) alone or in combination annually, buy, receive for commercial purposes, sell or share the personal information of 50,000 or more consumers, households or devices; or (C) derive 50 percent or more of their annual revenue from selling consumers' personal information. Any entity that controls, or is controlled by, a company meeting the above description and shares common branding with that entity is also covered.

NIS: The more specific requirements of the Directive, as put into place by Member States, will effectively apply to two types of entities: operators of essential services (OES) and digital service providers (DSP). Each Member State will determine what types of organizations fall into each category. OESs are organizations operating in vital sectors as specified by each Member State. Vital sectors generally include energy, transport, banking, finance, health, water or digital infrastructure. DSPs are organizations that provide a digital service, including search engines, online market places and cloud computing services.[7]

Covered Data

GDPR: The GDPR generally applies to the processing of personal data, which is any information relating to an identified or identifiable natural person, or a "data subject." Guidance from the Article 29 Working Party provides specific examples of the types of information that may fall within this broad definition, including things like IP addresses and GPS coordinates.[8] Additional protection is afforded under the GDPR for "sensitive data"[9] or personal data that reveals information about a data subject's ethnicity, religion, sexuality, etc.[10]

APEC: The APEC Framework generally applies to personal information on individuals (natural, living persons) in the various APEC member countries. "Personal information" is defined as information about an identified or identifiable individual, as well as information that would not meet this criterion alone, but, when put together with other information, would identify an individual. The APEC Framework has limited (if any) application to publicly available information.[11]

6 Doing business in this context means that a business located outside of California actively engages in a transaction for the purpose of financial or pecuniary gain or profit in California.

7 The NIS Directive contains certain exemptions for businesses that might otherwise fall within this definition, but that have fewer than 50 employees or less than €10 million in gross revenue.

8 Recital 30 of the GDPR also specifies that natural persons may be associated with online identifiers provided by their devices, applications tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.

9 We use the term "sensitive data" to refer to what the GDPR has determined are "special categories of personal data."

10 Sensitive data is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning a data subject's sex life or sexual orientation, certain health data, certain genetic data and biometric data if processed for the purpose of uniquely identifying a natural person.

11 Publicly available information under the APEC Framework means information that an individual knowingly makes or permits to be made available to the public, or that is legally obtained and accessed from (1) publicly available government records, (2) journalistic reports, or (3) information required by law to be made available to the public.

CCPA: The CCPA generally applies to consumers' (meaning residents of California) personal information. Personal information under the CCPA includes any information that relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA's expansive definition of personal information includes (1) personal identifiers; (2) characteristics associated with protected classifications, as provided for by California or federal law; (3) commercial information (records of personal property, products or services purchased, or consumption tendencies); (4) biometric information; (5) geolocation data; (6) audio, electronic, visual, thermal, olfactory or similar sensory information; (7) professional or employment-related information; (8) educational information; and (9) any inferences drawn from any of the information identified to create a profile about a consumer. The CCPA generally does not apply to publicly available information.[12]

NIS: The NIS Directive does not cover this issue.

Lawful Basis for Processing/Using Information

GDPR: Under the GDPR, a controller may process an EU data subject's personal data only if it meets one of the six lawful bases for doing so. Three of those bases are particularly relevant here: (1) for the performance of, or for entry into, a contract with a particular data subject; (2) to comply with a legal obligation to which the controller is subject under EU or Member State law; or (3) for the purposes of legitimate interests pursued by the controller or third party (except as overridden by the interests or certain rights and freedoms of the data subject). Absent another lawful basis, a controller can lawfully process personal data only if it can obtain express consent from the data subject. Consent must be freely given, specific, informed and unambiguous. It must be as easy for a data subject to withdraw consent as it is to give it.

12 Publicly available information under the CCPA means information that is lawfully made available from federal, state or local government records, but excludes biometric information collected without a consumer's knowledge and personal information used for a purpose different from the one for which the data is maintained and made available in the government records or otherwise publicly maintained.

APEC: Under the APEC Framework, personal information should be obtained in a fair and lawful manner; where appropriate, individual notice or consent should be provided or obtained regarding that collection, and only so much personal information should be collected as is relevant to the purposes for which it is being collected. Personal information that has been collected should be used to fulfill only the purposes, or closely related purposes, for which it was collected, unless one of the following three exceptions applies: (1) an individual consents to the PIC's use of personal information for additional purposes; (2) use of the information is necessary to provide the individual with a product or service requested by the individual; or (3) laws, legal proclamations or legal instruments authorize the use of information for purposes beyond those specified during the initial collection.

CCPA: The CCPA, unlike the GDPR or the APEC Framework, does not restrict the actual collection of that data. Rather, it focuses on giving consumers information about the collection and use of their data.

NIS: The NIS Directive does not consider this issue.

Requirement to Provide Information and Access to Data

GDPR: Under the GDPR, controllers must provide certain specified information to data subjects at the time that personal data is obtained. Data subjects must be provided at minimum with the following: (1) the purpose of the processing, (2) the categories of recipients that receive their data, (3) whether data is transferred out of the EU and related safeguards, (4) the period that data is retained (5) and an overview of their rights. They should also be provided with general information on how their information is processed and, if they ask, a copy of their personal data maintained by the controller.

APEC: Pursuant to the APEC Framework, individuals should be granted the right to (once they verify their identity) (1) know what information, if any, is being collected about them; (2) challenge the accuracy of the personal information that is collected about them; and (3) where appropriate, have their personal information rectified, completed, amended or, in some cases, entirely deleted. The ability to access and correct

personal information is not an absolute right under the APEC Framework. Rather, it must be balanced against the legitimate needs of the PIC or public entity that is collecting the information. This is a similar approach to that taken by the GDPR and the CCPA. A PIC is not required to provide an individual with information under the APEC Framework where doing so would violate the privacy of persons other than the requester. PICs are required to provide individuals with requested information (assuming that they are under an obligation to do so) within a reasonable time and in a reasonable form that is generally understandable.

CCPA: Under the CCPA, consumers have a right to request and receive (once the business verifies their request) (1) the categories and specific pieces of personal information that the business has collected about them, (2) the categories of sources from which the personal information is collected, (3) the business purposes for which the personal information is collected, (4) the categories of third parties with which the business shares consumers' personal information and (5) the categories of personal information that the business sold or disclosed about the consumer for a business purpose. The CCPA requires that a business provide a consumer with information for the 12-month period preceding the consumer's request.[13]

NIS: The NIS Directive does not consider this issue.

Right to Erasure/Deletion and to Rectification

GDPR: The GDPR grants data subjects two corresponding rights related to correcting or erasing their data: the right to correct inaccurate, or add to incomplete, personal data (right to rectification), and the right to erase personal data (right to erasure). There are six exceptions that permit companies to avoid erasure.[14] In addition, personal data must be erased immediately if the data are no longer needed for their original purpose, the data subject has withdrawn consent, the data subject has objected or erasure is required to fulfill a statutory obligation.

APEC: As previously noted, the APEC Framework empowers individuals to both request access to their personal information and correct their personal information. A PIC need not comply with an individual's request where (1) the individual does not verify his or her identity, (2) the cost or burden to the PIC would be disproportionate to the risk presented to the individual, (3) the PIC is required, or permitted, by law to retain the information; (4) disclosure could present legal or security risks to the PIC, including dissemination of confidential commercial information; or (5) compliance could violate the privacy of persons other than the requester. Where the PIC possesses a lawful and justifiable basis for denying an individual's request, it is required to provide the individual with an explanation as to its basis for denial and how the individual can challenge the denial. No explanation is necessary where providing an explanation would, by itself, violate a law or other judicial order.

CCPA: The CCPA grants certain consumers the right to request and have (if the request is verified) their personal information deleted. Businesses that do so must also direct service providers to do the same. There is no independent requirement that businesses delete consumer data absent receipt of a consumer request. There is no right to correct or add to information.

NIS: The NIS Directive does not cover this issue.

13 Reading the CCPA as it is now worded suggests that businesses may need to have processes and systems in place to provide such information as of January 1, 2019 (12 months before the CCPA takes effect).

14 Under the GDPR, the right to erasure does not apply if the processing of the personal data in question is necessary (1) to exercise the right to freedom of expression; (2) to comply with a legal obligation; (3) for the performance of a task that is carried out in the public interest or in the exercise of official authority; (4) for reasons of public interest in the area of public health; (5) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes; or (6) for the establishment, exercise or defense of a legal claim.

Explicit and Implicit Record-Keeping Requirements

GDPR: The GDPR generally requires that controllers maintain records of all processing activities for set periods. Those records must be provided to relevant regulators upon request.

APEC: Under the APEC Framework, personal information controllers are obligated to maintain records in a complete and accurate manner, and should keep them as up-to-date as is necessary to fulfill the purposes of use.

CCPA: The CCPA implicitly requires businesses to maintain records tracking what information is collected about consumers, the sources of that information, where that information is transferred, etc., to ensure that they are able to fully respond to consumer or regulatory requests. The CCPA also mandates that consumers are entitled to requested information for the 12-month period preceding their request, which implicitly requires that businesses hold information subject to such requests for a minimum of 12 months.

NIS: The NIS Directive requires, at a minimum, that OESs be able to provide the information necessary to assess the security of their network and information systems, including documented security policies. OESs must also maintain evidence of the effective implementation of security policies, including security audit results. Member States will likely add detail to these recordkeeping requirements as the Directive is transposed into national law.

Requirement to Implement Reasonable and Adequate Security

GDPR: The GDPR promotes a risk-based approach with regard to security. Personal data has to be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing, accidental loss, and destruction or damage. Entities are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk at issue. Among other things, the GDPR requires controllers to carry out data protection impact assessments if they undertake a type of processing that is likely to result in a high risk to the rights and freedoms of data subjects.[15] The GDPR also adopts the principles of data protection by design and data protection by default, which are intended to force companies to build data protection concepts into their systems.

APEC: Under the APEC Framework, PICs are expected to implement appropriate security safeguards in order to protect the personal information they hold against known or anticipated risks (e.g., loss, unauthorized access, destruction or modification). The safeguards are expected to be proportionate to the likelihood and the severity of the threatened harm, the sensitivity of the information at issue and the context in which the information is being held. The APEC Framework requires that security controls be subject to periodic review and assessment.

CCPA: The CCPA implicitly requires businesses to adopt reasonable security measures by empowering consumers to bring private rights of action against businesses that fail to do so and that suffer security incidents involving nonencrypted and nonredacted personal information.[16] Other California statutes explicitly require businesses that own, license or maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the type of information at issue. Under the CCPA, businesses sharing personal information with third parties must ensure that reasonable security requirements are included in contractual provisions.[17] California has not officially defined what constitutes reasonable security, but the California Attorney General's Office previously suggested that the 20 controls in the Center for Internet Security's Critical Security Controls may constitute a "minimum

15 Such a high risk is likely to result where the processing entails: (1) an evaluation or scoring, including profiling and predicting, of aspects specific to a data subject; (2) automated decision making; (3) the systematic monitoring of data subjects, including in publicly accessible areas; (4) the potential transfer of data out of the EU; or (5) the innovative use of data.

16 The CCPA, moreover, rewards companies by limiting some types of liability if they adopt certain reasonable security best practices like the pseudonymization of data, use of data in the aggregate, encryption of data or redaction of personal information.

17 *See, e.g.*, Cal. Civ. Code § 1798.81.5(b), (c).

level of information security that all organizations that collect or maintain personal information should meet."[18]

NIS: The NIS Directive requires that OESs and DSPs take appropriate and proportionate security measures to manage risks to their networks and information security systems, including by implementing organizational cyber resilience programs. What constitutes appropriate and proportionate security awaits further clarification by Member States as they transpose the Directive into national laws. It is likely that these terms will be treated in much the same manner as "appropriate" or "reasonable" security and will vary by industry and the type of risk at stake.

Transfer or Sale of Data/Information and Vendor/Service Provider Issues

GDPR: The GDPR requires that controllers closely oversee their processor's compliance with it. Controllers may use only processors that agree to abide by the GDPR's safeguards in a written contract or through another legally enforceable mechanism. There are strict requirements as to what must appear in that contract or agreement. Responsibility for oversight of GDPR compliance flows down through the processor-subcontractor hierarchy. Processors must require subcontractors engaged in processing activities to similarly attest to their compliance with the safeguards promised by the processor in its contract with the controller.

APEC: Unlike the GDPR, the APEC Framework applies to the conduct of only PICs. It does not apply to processors or subprocessors. This is similar to the pre-GDPR regulatory environment in the EU. Various efforts have spurred the development of informal rules and processes that help PICs implement adequate security and notification controls with regard to their processors, and that assist processors in demonstrating their compliance with the requirements generally expected of PICs with regard to safeguarding information processing. Although these movements are helpful, none has yet changed the fact that the ultimate burden for any violation of the APEC Framework (even if committed by a processor) lies with PICs.

18 California Attorney General's Office, California Data Breach Report (Feb. 2016), p. v.

CCPA: The CCPA also applies to the transfer of personal information between entities, including to subsidiaries, "service providers" or third parties.[19] There must be a written contract governing the sale or sharing of personal information for an entity to be considered a service provider. Any entity that is not a "business" or a "service provider" as defined in the CCPA is considered a third party. Whether an entity is a service provider or a third party matters, since the CCPA limits a business's liability for service provider misconduct if certain conditions are met (it does not do so for third parties), and limits a business's ability to sell, share or disclose consumers' personal information to third parties without providing consumers with prior notice and the option to opt out of the sale (not required for service providers). Certain restrictions apply once a consumer opts out of the sale or sharing of their information. Children under the age of 16 must affirmatively opt in to the selling or sharing of their information, either through their legal guardians (if younger than 13) or by themselves (if between 13 and 16).

NIS: Specifics on this issue will likely be included in national laws used to transpose the NIS Directive into local laws.

Notification Requirements

GDPR: The GDPR requires controllers to provide relevant regulators with notice of personal data breaches without undue delay and no later than 72 hours after becoming aware of the breach.[20] This 72-hour notice requirement mimics similar requirements found in other statutes.[21]

19 "Service providers" are any for-profit entity that processes information for a business-related purpose pursuant to a written contract with a business to which the CCPA applies.

20 A personal data breach, for the purposes of the GDPR, is a breach of security (1) where the confidentiality of the data subjects' data is compromised; (2) where the integrity of the personal data at issue is compromised; or (3) where the availability of the system is sufficiently affected, even if the underlying data on the system may not have been affected or accessed.

21 For example, the New York Department of Financial Services requires that covered entities notify the Department "as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred," either where notice of the event is required to a certain government or similar supervisory body or where the event has a reasonable likelihood of materially harming the entity's operations. 23 N.Y.C.R.R. § 500.17(a).

APEC: The APEC Framework does not directly address data security breaches and does not specifically require breach notification, but its general principles support providing notice. In 2015, moreover, APEC member countries adopted the Cross-Border Privacy Rules (CBPR), which mandate that member countries impose rules to require PICs to contractually obligate processors, agents, contractors or other service providers to notify PICs of any breach or data security incidents. The CBPRs do not require that PICs provide mandatory notice of breaches or data security incident to the authorities or individuals. Member countries are free to adopt such requirements on their own.

CCPA: The CCPA does not impose notification requirements on businesses. That requirement appears in California's general data breach statute, which requires that notice be provided to state regulators if 500 or more California residents are affected by a breach. Notice must be provided in as expeditious a time as possible and immediately following a breach.[22]

NIS: Both OESs and DSPs must notify relevant national authorities of serious security incidents "without undue delay."[23] Member States are free to modify this requirement when they transpose the Directive into their national laws. By November 9, 2018, Members States must provide the European Commission with a list of the companies that would be required to report cyberattacks under their national laws.

Enforcement Mechanisms, Penalties and Oversight

GDPR: The GDPR provides for both public and private enforcement. Regulatory actions can arise from data subjects' complaints, from regulatory inquiries, etc. Fines tied to regulatory matters can range from, for more serious violations, €20,000,000 or up to 4 percent of the total worldwide annual turnover of the preceding financial year.[24] In addition, fines may also be imposed on the parent company of the fined controller or processor. Multiple violations may lead to several administrative fines being applied. Data subjects may pursue private rights of action if they can establish (1) material or nonmaterial damages, (2) unlawfulness, (3) causation and (4) fault. The GDPR permits data subjects to assign their rights to pursue private enforcement to not-for-profit protection organizations, which can bring representative actions on behalf of a number of data subjects (akin to a class action in the United States).

APEC: Enforcement of the APEC Framework is left to member countries' Privacy Enforcement Authorities (PEAs) and is pursued in a manner consistent with the way in which the APEC Framework's principles were transposed into the relevant country's national laws. APEC established the Cross-Border Privacy Enforcement Arrangement (CPEA) as a multilateral arrangement to facilitate cooperation between members' PEAs. CPEA promotes the voluntary sharing of information, cross-border referrals, and parallel or joint enforcement actions. Participation in CPEA is a prerequisite to participation in the CBPR system.

CCPA: As with the GDPR, the CCPA permits both public and private enforcement. The California Attorney General has the sole right to pursue civil penalties against businesses through a civil action in the public's name. Statutory penalties of up to $2,500 for general violations or $7,500 for intentional violations are available on a per-violation basis. Consumers may pursue a private enforcement action only if their non-encrypted or non-redacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a business's failure to implement and maintain reasonable security. Consumers may seek, among other things, the greater of either their actual damages or damages in an amount not less than $100 and not greater than $750 per consumer per incident.

22 *See* Cal. Civ. Code § 1798.82.

23 A serious security incident in this context really means an incident that could significantly affect the continuity, availability and integrity of the service provided by the entity. Determining the relative significance of any potential risk requires a multifactor analysis.

24 This range of fines applies if entities violate any one of six provisions as provided for in Article 83(5) and (6).

NIS: Failure to comply with the national laws adopting the NIS Directive can lead to expensive regulatory investigations and hefty fines. The NIS Directive envisions that competent authorities will be empowered to audit OESs to evaluate their compliance. DSPs, in contrast, will only be subject to the scrutiny of competent authorities if there is a complaint regarding their compliance or following a security incident. The Directive does not anticipate private rights of action. Each Member State is responsible for setting its own cap on the maximum fine that may be imposed for violations. To date, the more onerous sanctions for violations of national laws transposing the NIS Directive may cost a company up to £17,000,000 (United Kingdom), or up to €5,000,000 or 10 percent of annual worldwide turnover, whichever is greater (Germany).[25]

25 The following are additional fines and penalties that have been transposed into national laws to date: (1) Cyprus – six months' imprisonment and/or up to €8,500; (2) Czech Republic – up to €200,000; (3) Estonia – up to €20,000; (4) Finland – existing sanctions as provided under prior law; (5) Germany – up to €5,000,000 or 10 percent of annual worldwide turnover, whichever is greater; (6) Slovakia – from €300 up to 1 percent of the entity's global annual turnover, provided that it does not exceed €300,000; (7) Sweden – from 5,000 to 10,000,000 Swedish Kroners (roughly €480 to 960,000); and (8) United Kingdom – up to £17,000,000.

Proactive Compliance Measures

Although the GDPR, the APEC Framework, the CCPA and the NIS Directive often diverge from one another, there are some general measures that those in the defense and aerospace industries can adopt to meet certain minimal compliance requirements that are common across these and other privacy and information security regimes. The following list provides proactive measures to implement to facilitate cross-regime compliance:

- **Understanding What You Have, Where You Have It and Why You Have It –** Whether for privacy or information security planning purposes, it is critical that an organization fully understand the what, where and why of its data universe. For larger companies, a key aspect of this exercise should be mapping all transfers of data outside the entity and logging all internal access to sensitive data.
- **Implementing an Appropriate, Industry-Recognized Information Security Framework to Ensure Adoption of Reasonable or Appropriate Security Measures –** The GDPR, the CCPA, the APEC Privacy Framework the NIS Directive, and a range of other privacy and information security-related statutes require companies to implement a risk-based approach to security and to implement security measures intended to assist in best addressing the particular risks associated with their industry. It is critical to both select a recognized framework to follow and fully incorporate that framework into policies and practices.
- **Drafting Strong Contracts to Limit Liability for Vendor and Subcontractor Vulnerabilities –** Both the GDPR and the CCPA require that companies have written contracts in place with the entities with which they intend to share data to ensure that those entities abide by the same protective measures as promised by the initial company. These provisions should place the burden on service providers and vendors to comply with key regulations and require indemnification related to these issues.
- **Creating Processes for Tracking Protected Information and Responding to Requests Related to the Same –** Even organizations that have undergone data mapping exercises do not necessarily have processes in place to track the collection of data related to a particular data subject or consumer, or to respond to inquiries about the same. Providing data on specific individuals is fast becoming a trend in privacy protection statutes.

- **Limiting the Collection of Data/Information to That Which Is Necessary –** As laws defining what constitutes protected data or information continue to expand, companies would be wise to collect only so much data as they actually need. Being strategic with collection can help protect companies down the road.
- **Planning for 72-Hour Notice in the Event of an Incident –** The deadlines by which companies have to provide notice to regulators following a security incident, including data breaches, continue to evolve and vary from jurisdiction to jurisdiction. A good rule of thumb is to plan and prepare to provide notice within a 72-hour window and take additional time as permitted in the specific jurisdictions affected.
- **Bolstering Internal Governance and Oversight of Privacy and Information Security Measures –** Given the liability and reputational issues at stake, organizations should consider adopting stronger internal governance mechanisms to ensure consistent oversight of the development and implementation of privacy and information security measures. Regulators are increasingly taking companies' governance measures into account when evaluating an organization's compliance efforts.
- **Updating External-Facing Privacy and Security Policies to Improve Compliance and Lessen Litigation Risks –** External-facing privacy and information security policies are often a key piece of evidence in regulatory or civil litigation related to incidents. Companies should consistently update those policies as they consider and adopt new procedures, industry-specific standards, etc.
- **Encrypting Data as a Matter of Course –** Multiple international and local U.S. statutes provide protection for data that, although affected by a security incident, was encrypted. Ensure that your organization is encrypting data when they are collected, stored or transmitted. Encryption has both security and privacy benefits for an organization.

For more information, please contact:

Scott M. Heimberg
sheimberg@akingump.com
+1 202.887.4085

Robert K. Huffman
rhuffman@akingump.com
+1 202.887.4530

Natasha G. Kohne
CIPP/US
nkohne@akingump.com
San Francisco
+1 415.765.9505

Akin Gump
STRAUSS HAUER & FELD LLP

Akin Gump Strauss Hauer & Feld LLP is a leading global law firm providing innovative legal services and business solutions to individuals and institutions. Founded in 1945 by Richard Gump and Robert Strauss with the guiding vision that commitment, excellence and integrity would drive its success, the firm focuses on building lasting and mutually beneficial relationships with its clients. Our firm's clients range from individuals to corporations and nations. We offer clients a broad-spectrum approach, with over 85 practices that range from traditional strengths such as appellate, corporate and public policy to 21st century concentrations such as climate change, intellectual property litigation and national security.