







IN THIS ISSUE

- 2  [Our Authors](#)
- 3  [Information Security in Government and Defense Contracting: New and Upcoming Requirements](#), by Berne Kluber
- 3  [Developing Cybersecurity Requirements in Banking, Insurance and Other Financial Services](#), by Theodore P. Augustinos
- 4  [CyberSECurity – The SEC Increases Data and System Protection Work](#), by Molly McGinnis Stine
- 5  [HIPAA Enforcement Update](#), by Ashley Wheelock and Tammy Woffenden
- 6  [Equifax Lax About Hacks, Says Shareholder Lawsuit](#), by Bilal Zaheer and Molly McGinnis Stine
- 6  [New York DFS Cybersecurity Regulation Update: Lots Left To Do](#), by Theodore P. Augustinos
- 7  [Are We Covered by the EU GDPR? – A Warning for U.S.-Only Businesses](#), by Thomas J. Smedinghoff and Elizabeth Kilburn
- 9  [Incident Response – Privilege and Work Product Issues After *In re Premera*](#), by Brandan J. Montminy and Molly McGinnis Stine

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

OUR AUTHORS:



Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com



Thomas J. Smedinghoff
Of Counsel
Chicago
312-201-2021
tom.smedinghoff@lockelord.com



Elizabeth Kilburn
Associate
London
+44 (0) 20 7861 9288
elizabeth.kilburn@lockelord.com



Ashley Wheelock
Associate
Austin
512-305-4860
ashley.wheelock@lockelord.com



Berne C. Kluber
Partner
Houston
713-226-1513
bkluber@lockelord.com



Tammy Ward Woffenden
Partner
Austin
512-305-4776
twoffenden@lockelord.com



Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com



Bilal Zaheer
Partner
Chicago
312-201-2875
bilal.zaheer@lockelord.com



Brandan Montminy
Associate
Dallas
214-740-8445
brandan.montminy@lockelord.com

Information Security In Government and Defense Contracting: New and Upcoming Requirements

By Berne Kluber

As many contractors know well, federal and defense acquisition processes can be a complicated, rule-intensive process subject to frequent change. Fortunately, some recent changes appear to be well designed to provide for greater protection of government contract information and defense-related information. Companies that regularly enter into federal government contracts and/or defense-related contracts should carefully review all regulations applicable to those practices, and take care to incorporate the below-described updates into their practices.

First Update – Federal Acquisition Regulation Basic Safeguarding of Contractor Information Systems

In May 2016, the Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics Space Administration (NASA, together with DoD and GSA, the "Agencies") issued a final rule, which is now in effect, imposing significant [new information security obligations](#) on government contractors by requiring the inclusion of: information security-related statements in written acquisition plans for certain contract types, highly-particularized information security-related language in contracting entities, and the inclusion of that same language in contractor agreements with subcontractors. Interestingly, the final rule is drafted with the eye on protection of information systems that may process, store, or transmit "Federal Contract Information," which is defined as "information, not intended for public release that is provided by or generated for the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, as necessary to process payments."

The most significant changes arise from the information security requirements that must be imposed in government contracts (and subcontracts). That requirement will, in effect, mean that government contractors (and their subcontractors) are required to implement safeguards including:

- limitations on system access (both with respect to personnel and transactions allowed to provide access to the systems);
- verifications and controls on connections to external networks;
- sanitation or destruction of media containing Federal Contract Information;
- limitation of physical access to systems;
- visitor escorts, monitoring, and audit logs;
- monitoring, controls, and protections for organizational communications;
- implementation of subnetworks for publicly accessible system components that are physically or logically separated from internal networks;
- timely identification, reporting, and correction of system flaws;
- protections from malicious code and updates to those protections.

Companies regularly engaged in governmental contracts should carefully review in-place practices to determine if they are able to comply with newly-imposed requirements, and review subcontractor engagement processes to ensure that they are in compliance with specific contracting requirements.

Second Update – NIST Special Publication (SP) 800-171 Compliance by December 31, 2017

In October 2016 the Defense Federal Acquisition Regulation Supplement (DFARS) was updated to require subject entities to implement information security requirements set forth in Special Publication 800-171 from the National Institute of Standards and Technology (NIST) - *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* - before December 31, 2017. DFARS 252.204-7008.

The information security requirements applicable to defense information systems include requirements as may be imposed by contract, and particular security and diligence requirements for use of cloud computing services. DFARS 252.204-7012(b).

Although many defense contractors already have significant information security controls in place, strict compliance with Special Publication 800-171 may involve changes to operational practices and careful examination of in-place policies. Special Publication 800-171 includes particular requirements with respect to access controls, awareness and training, audit and accountability, configuration management, identification and multi-factor authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and system and information integrity. Contractors must submit requests for variances from Special Publication 800-171 for review by the CIO of the Department of Defense. DFARS 252.204-7012.

Perhaps most notably, DFARS now imposes an incident reporting requirement such that contractors must report "a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract" within 72 hours via an online portal provided by the Department of Defense. DFARS 252.204-7012(c).

Defense contractors and subcontractors that are registered with the Department of State, Directorate of Defense Trade Controls (DDTC) should consider submitting a voluntary disclosure to DDTC if a cyber incident includes the potential release of technical data (as defined in the International Traffic in Arms Regulations (ITAR)).

Developing Cybersecurity Requirements in Banking, Insurance and Other Financial Services

By Theodore P. Augustinos

The financial services industry has been dealing with requirements for cybersecurity since 1999, but 2017 brought new, significant, and proliferating obligations. The bar for the whole industry was clearly raised by the unilateral action of the New York Department of Financial Services (DFS), which adopted a new regulation, Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500), effective March 1, 2017. The DFS Cybersecurity Regulation imposes significant new responsibilities on DFS licensees (which include insurers and producers, banks, mortgage lenders and brokers, and others) over a transition period ending in 2019.

Taking up the mantle, the National Association of Insurance Commissioners (NAIC), which had been working on a model information security law for two years, essentially scrapped its prior drafts and, in October 2017, adopted much of the terminology and concepts of the DFS Regulation to promulgate a model law that would not create substantial inconsistencies with the DFS. In fact, a drafter's note to the NAIC Model specifies that compliance with the DFS Regulation would be deemed compliance with the NAIC Model. There are, however, important differences and distinctions between the two regimes, and it is certainly possible that states will adopt the NAIC Model with their own revisions that could create additional inconsistencies. Any such revisions would complicate compliance, and drive up the cost.

The NAIC Model, if and as adopted into law by the various states, would apply to licensees of state insurance regulators. The DFS Regulation applies to all DFS licensees (as well as those required to obtain DFS permits, registrations, and other authorizations), including licensees in the insurance, banking and other financial services industries, but does not include securities firms, which are not in New York licensed by the DFS. It is interesting to note that the Colorado Division of Securities and the Vermont Securities Division have adopted regulations, similar in many respects to New York's, but specific to the securities industry. Between the NAIC Model and other state initiatives, technical cybersecurity requirements for the financial services industry may certainly be expected to multiply. Even for financial services participants outside the insurance industry, and for those in jurisdictions that may not take immediate action to adopt the NAIC Model, a review of the new requirements would be well-advised, as the themes, if not the actual technical requirements, should be addressed in any serious cybersecurity program.

The following is a description of some of the critical provisions of the DFS Regulation and the NAIC Model, and the differences and nuances between them.

1. **Information Security Program.** Both the DFS Regulation and the NAIC Model require the adoption of an Information Security Program (called a Cybersecurity Program in the DFS Regulation) to govern the protection of data and systems. One of the important developments of the DFS Regulation and the NAIC Model is the recognition that cybersecurity must go further than protection of personal information, and must protect certain business and operating, as well as information, systems. Both the NAIC Model and the DFS Regulation contemplate that the program should take into account the size and sophistication of the licensee, and the nature of its risks, although the NAIC Model is more explicit on this point.
2. **Risk Assessment.** Under both regimes, the Information Security Program itself, and the other, related policies and procedures, are to be based on a risk assessment. The DFS Regulation is far more specific on the technical requirements for a risk assessment, including that it must be conducted in accordance with written policies and procedures.
3. **Qualified and Trained Personnel.** As cybersecurity cannot be addressed with exclusively technical solutions, and as human error plays so prominently as a cause of compromises, both the DFS Regulation and the NAIC Model impose responsibilities related to personnel. The DFS obligations concerning personnel are far more exacting and onerous, but both require the designation of a specific person to be responsible for cybersecurity, and the implementation of awareness training for all personnel.
4. **Access Control.** A key element of any cybersecurity program, controlling access to information systems is a specific requirement of both the DFS Regulation and the NAIC Model.
5. **Encryption.** While the NAIC specifically requires encryption only of certain data transmitted over a public network, and stored on laptops and other mobile devices, the DFS Regulation also requires encryption of data at rest (e.g., on desktops and servers, or in storage), with some flexibility for compensating controls where encryption is not feasible.
6. **Notification of Certain Cybersecurity Events.** Consistent with the new European regime under the General Data Protection Regulation, both the DFS Regulation and the NAIC Model require notification to the regulator of certain compromises of data and systems within 72 hours. Both also leave the obligation to notify affected individuals and other parties to the general breach notification statutes. The NAIC Model also requires 72 hour notice by reinsurers to ceding insurers, and under certain circumstances to producers of record.
7. **Annual Certification of Compliance.** Under both the DFS Regulation and the NAIC Model, annual certificates of compliance must be filed with the regulator. It is important to note, however, that the certification requirement of the NAIC Model applies only to insurers, and not to other licensees such as producers and others.
8. **Exemptions.** Both the DFS Regulation and the NAIC Model contain exemptions for certain reinsurers, captives and others, but the DFS Regulation contains several additional, important exemptions. For example, while the NAIC Model would exempt licensees with fewer than 10 employees, the small business exemption of the DFS Regulation also contains an asset and revenue threshold below which a business is exempt. This could reflect the fact that the NAIC Model has expressly provided that its obligations are to be based on the size and sophistication of the licensee; the DFS Regulation has less built-in flexibility. It is important to note that the DFS exemptions for certain covered entities are only partial, and still require compliance with significant elements of the DFS Regulation. The NAIC Model exemptions are self-executing, while several of the exemptions under the DFS Regulation require the filing of a notification of exemption.

CyberSECurity – The SEC Increases Data and System Protection Work

By Molly McGinnis Stine

The U.S. Securities and Exchange Commission is at the center of the current day "cyber storm" of data and system protection, both as a victim and as a regulator. According to an SEC [director](#), "[c]yber-related threats and misconduct are among the greatest risks facing investors and the securities industry."

The SEC recognizes that it is itself vulnerable. It recently [acknowledged](#) that its EDGAR records system was subject to a data breach, and information obtained through that breach may have been exploited for purposes of illicit trading.

But the SEC has also sharpened its focus on the cybersecurity of itself and the entities it regulates. The SEC Chairman Jay Clayton plainly [stated](#) in September 2017 that "[c]ybersecurity is critical to investors, market participants, our markets, and the Commission itself. By promoting effective cybersecurity practices in connection with both the Commission's internal

operations and its external regulatory oversight efforts, it is our objective to contribute substantively to a financial market system that recognizes and addresses cybersecurity risks and, in circumstances in which these risks materialize, exhibits strong mitigation and resiliency.”

In pursuit of a safer financial market system, the SEC has recently taken some substantive [steps](#). It has launched a “Cyber Unit” in its Enforcement Division and created a Retail Strategy Task Force that “will develop proactive, targeted initiatives to identify misconduct impacting retail investors.”

The SEC has also continued to gather empirical information from its regulated entities as shown in a recent set of [Observations from Cybersecurity Examinations](#) released by its Office of Compliance Inspections and Examinations. These Observations make clear that the SEC expects to see not only information security policies but also regular follow-through.

Also, the SEC’s director of corporation finance recently advised, according to [news accounts](#), that public companies will be seeing new guidance for the reporting of cybersecurity incidents. He did not indicate a timetable. The SEC previously published [guidelines](#) in October 2011 that confirm that companies should treat cybersecurity issues as a risk factor in assessing whether, when and what to disclose.

Companies already face any number of legal, regulatory and business reasons to be vigilant in their cybersecurity. Escalation of the SEC’s involvement will add to those reasons.

HIPAA Enforcement Update

By Ashley Wheelock and Tammy Woffenden

With respect to enforcement, the Department of Health and Human Services, Office for Civil Rights (OCR) announced two Settlement Agreements to resolve allegations of HIPAA violations between May and October of 2017. Neither settlement resulted from large breaches but instead focused on discrete incidents involving impermissible disclosures of PHI. These Settlement Agreements demonstrate that OCR will take into account aggravating factors including the egregious nature of the disclosure, extent of the harm caused to the affected individual(s), and lack of institutional safeguards protecting the information.

On May 23, 2017, OCR publicized that St. Luke’s Roosevelt Hospital Center Inc. (St. Luke’s) entered into a [Resolution Agreement and Corrective Action Plan](#) to resolve impermissible disclosures of two patients’ PHI. St. Luke’s operates the Institute for Advanced Medicine, formerly the Spencer Cox Center for Health (Spencer Cox Center), which specializes in the treatment of HIV positive and AIDS patients. OCR received a complaint that a Spencer Cox Center employee accidentally faxed an HIV positive patient’s PHI to the patient’s employer. During the course of the complaint investigation, OCR discovered that the Spencer Cox Center also impermissibly released similar sensitive health information in a different incident nine months prior but had failed to address vulnerabilities in its compliance program. Given the sensitivity of information involved, including the patients’ HIV status, sexual orientation, and mental health diagnoses, the disclosures were noted to be especially “egregious.” St. Luke’s agreed to pay \$387,200 to resolve the allegations, and the Corrective Action Plan requires St. Luke’s reevaluate its staff training materials related to HIPAA. When announcing the settlement, OCR Director Roger Severino noted

that “[i]n exercising its enforcement authority, OCR takes into consideration aggravating factors such as the nature and extent of the harm caused by failure to comply with HIPAA requirements” and reminded both covered entities and business associates that they have the responsibility under HIPAA to both identify and actually implement safeguards to protect sensitive data.

On May 10, 2017, OCR announced a \$2.4 million [Resolution Agreement](#) in connection with a hospital press release that impermissibly identified a patient by name. The patient presented an allegedly fraudulent identification card to Memorial Hermann Health System’s (Memorial) office staff, which resulted in the patient’s arrest. Thereafter, Memorial issued a press release disclosing the patient’s name to multiple media outlets. In addition to the monetary settlement, Memorial agreed to adopt a comprehensive Corrective Action Plan requiring it to update its policies and procedures on safeguarding PHI from impermissible disclosures, including releases to the media. Although HIPAA permits organizations to disclose PHI to law enforcement, the law enforcement exceptions do not extend to public disclosure of PHI, even when criminal activity occurs.

On October 27, 2017, OCR responded to President Trump’s call to action to combat the nation’s opioid crisis by issuing clarifying [guidance](#) regarding the release of information in medical emergencies, such as during an opioid overdose, without violating the HIPAA Privacy Rule. HIPAA allows health care professionals to disclose some health information without a patient’s authorization under certain circumstances, including sharing health information with family and close friends if the provider determines that doing so is in the best interests of an incapacitated or unconscious patient and the information is directly related to the family or friend’s involvement in the patient’s health care or payment of care. For example, the guidance states that a doctor whose patient has overdosed on opioids is presumed to have complied with HIPAA if the doctor informs family, friends, or caregivers of the opioid abuse after determining, based on the facts and circumstances, that the patient poses a serious and imminent threat to his or her health through continued opioid abuse upon discharge. Furthermore, OCR takes the position that decision-making incapacity may be temporary and situational and does not have to rise to the level where another decision-maker has been or will be appointed by law. The guidance also notes that HIPAA allows health care providers to disclose information to persons who are in a position to prevent or lessen a serious and imminent threat to a patient’s health or safety. Importantly, a health care provider is not permitted to share health information about patients with the capacity to make their own health care decisions (and who object to the provider sharing the information) unless there is a serious and imminent threat of harm to the patient’s health.

Equifax Lax About Hacks, Says Shareholder Lawsuit

By Bilal Zaheer and Molly McGinnis Stine

In early September, Equifax disclosed a now well-known data breach that ultimately affected a reported 146 million customers in the United States. The breach allegedly occurred in May 2017, as a result of an online security flaw known to the company by March 2017 but that was not properly fixed. In late July, the company noticed suspicious traffic on its system. Ultimately, the breach was discovered, and the software flaw addressed, but not before the names, addresses, social security numbers and other

personal information of millions of customers were stolen. The stock market's reaction to the news of the Equifax data breach was immediate – the company's share price plunged over 15% within days of the announcement.

That led to a group of Equifax shareholders quickly filing a class action against the company, its (now former) CEO and its CFO in a Georgia federal district court, alleging fraud under federal securities laws and seeking to recover damages. The [complaint](#) alleges, among other things, that "(1) the Company failed to maintain adequate measures to protect its data system; (2) the Company failed to maintain adequate monitoring systems to detect security breaches; (3) the Company failed to maintain proper security systems, controls and monitoring systems in place; and (4) as a result of the foregoing the Company's financial statements were materially false and misleading at all relevant times."

To date, shareholder lawsuits in the wake of data breaches, especially suits alleging securities fraud claims, have been relatively rare. And as we noted [previously](#), derivative lawsuits filed to date have not fared well in court, with most having been dismissed in the initial stages.

The circumstances of the Equifax breach could make this case different. To begin with, one of the reasons shareholders have generally not filed securities class actions after a data breach is that the affected company did not experience a meaningful drop in share price and so there were insufficient damages to pursue in litigation. Here, Equifax's stock price dropped 15% the day after the breach was announced and dropped even further in the week after the announcement. The current stock price remains below the price prior to disclosure of the incident.

In addition, media reports indicate that three Equifax executives sold their company stock shortly after the company discovered the security breach but before the breach was disclosed to the public. The amount of stock sold was about \$2 million. A special committee comprised of independent board members has investigated the stock sales and recently issued a report stating that the executives were unaware of the breach at the time they sold their stock. Nevertheless, sufficiently supported shareholder allegations to the contrary could be enough to take a case into the discovery phase.

Finally, the seriousness of the breach (nearly half of all Americans affected), combined with the fact that Equifax's business is based on securing and protecting customer information, may lay the groundwork for a derivative lawsuit claiming breach of fiduciary duty against Equifax's directors and officers that could survive the initial pleadings hurdles that stymied similar lawsuits brought against directors and officers of Target, Wyndham and Home Depot (no such lawsuit against Equifax directors and officers has been filed yet).

As of the date of this article, derivative lawsuits against directors and officers of Wendy's and Yahoo!, seeking damages in connection with data breaches experienced by those companies, remain pending. Moreover, a derivative lawsuit against Home Depot that was initially dismissed on the pleadings recently settled for \$1.125 million after the shareholders sought to appeal dismissal. Thus, it remains worthwhile to keep an eye on the progression of these lawsuits.

New York DFS Cybersecurity Regulation Update: Lots Left To Do

By Theodore P. Augustinos

Insurers and producers, banks, lenders and others licensed by the New York Department of Financial Services (DFS) have already had to comply with several of the requirements of the new DFS Cybersecurity Regulation, but for most, there's a lot left to do. For the financial services and insurance industries, the Regulation has far reaching implications, affecting many DFS licensees (Covered Entities) and requiring significant planning and effort from the time of the Regulation's effective date of March 1, 2017 through the last transition date of March 1, 2019 and beyond.

From the time of the Regulation's effective date, Covered Entities needed to take immediate action to meet its various compliance requirements, which started transitioning into effect on August 28, 2017. Even Covered Entities subject to one of the limited exemptions must satisfy many of the Regulation's new requirements, and even employees, agents and others who are covered by the information security program of an employer or principal had to file for an exemption.

August 28, 2017 and October 30, 2017: Hopefully, You Were Prepared.

By the first transition date of August 28, 2017, most Covered Entities had to satisfy the following requirements:

- Cybersecurity Program must be maintained;
- Cybersecurity Policy must be drafted and implemented;
- Chief Information Security Officer must be designated (unless subject to a limited exemption);
- Access Privileges must be limited;
- Cybersecurity Personnel must be engaged, trained and updated (unless subject to a limited exemption);
- Incident Response Plan must be drafted and established (unless subject to a limited exemption); and
- Notices to Superintendent of certain cybersecurity incidents will be required.

Are you subject to one of several potential exemptions? If so, you should have filed your Notice by October 30.

As noted above, even Covered Entities subject to one of the limited exemptions, and employees and others, must file a Notice of Exemption, which is due within 30 days after a determination that the exemption applies. DFS has interpreted this requirement to mean that Covered Entities subject to one of the exemptions at the time of the first transition date (August 28) were required to file by September 27, 2017, which was later extended to October 30.

February 15, 2018: The First Annual Compliance Certificate.

A significant requirement of the Regulation is that a Senior Officer (as defined by the Regulation) or the Board of Directors must, on behalf of the Covered Entity, certify that the Covered Entity is in compliance with all applicable requirements of the Regulation. It is important to note that if a Covered Entity cannot certify that all of the applicable requirements are satisfied, the Covered

Entity cannot file the compliance certificate; no exemptions may be taken. (Note that requirements are only covered by the compliance certificate once the applicable transition date has passed.) As the individual or individuals making the certification, which is to be submitted electronically on a prescribed form, will need to be identified, and satisfied that the certificate is truthful, this requirement should be part of the planning starting now, and not left until the deadline.

March 1, 2018: What to Focus on Next?

By the next transition date of March 1, 2018, each Covered Entity will need to have completed its first periodic risk assessment under written policies and procedures, and document its findings. In addition, Covered Entities other than those subject to a limited exemption must meet the following requirements of the Regulation:

- First annual requirement for CISO's report to the Board;
- Continuous monitoring, or periodic penetration testing and vulnerability assessments;
- Multi-factor authentication or risk-based authentication; and
- Cybersecurity awareness training for all personnel.

September 3, 2018: Most of the Rest.

Most of the remaining requirements of the Regulation must be satisfied by September 3, 2018, except the requirement to draft and implement written policies and procedures to manage security risk presented by third-party service providers, for which the transition date is March 1, 2019. Covered Entities must, by September 3, 2018, draft and implement policies and procedures limiting the retention of certain data, and providing for its secure disposal. In addition, Covered Entities other than those subject to a limited exemption are required by September 3 to:

- Establish and document an audit trail able to recreate material financial transactions and to detect and respond to certain cybersecurity events;
- Draft and implement policies for security of applications used within tech environment;
- Monitor activities of authorized users; and
- Satisfy encryption requirements.

Looking Past March 1, 2019: The Last of the Transition Dates is NOT the End of the Project.

Even after the last transition date of March 1, 2019, at which time the third-party service provider requirements (as well as all other applicable provisions of the Regulation) will be fully operational, Covered Entities will not be finished with their efforts to comply with the DFS Cybersecurity Regulation. Several requirements of the Regulation will require ongoing and continuous or periodic attention, including the requirements for risk assessments, penetration testing and vulnerability assessments, monitoring and training of employees, reports to the Board of Directors, filings of compliance certificates and notices of certain cybersecurity events.

In addition, it is important to note that several of the policies to be developed and implemented pursuant to the Regulation are to be based on the periodic risk assessment. As the risk assessment is to be conducted periodically, and as the results will change over time, the policies and procedures to be based

on the risk assessment will need attention, modification and refinement on an ongoing basis.

In addition, as evidenced by recent developments by the NAIC to develop a model cybersecurity law based on the DFS Regulation, and by the new effort in Colorado that applies to securities firms, new and additional requirements will certainly be imposed by other regulators and jurisdictions, potentially requiring additional, state-specific attention by Covered Entities licensed in other jurisdictions.

There is still a lot left to do to comply with the New York Department of Financial Services Cybersecurity Regulation, and this is a project that, for most Covered Entities, will not end.

A version of this article appears in the December issue of Intellectual Property and Technology Law Journal.

Are We Covered by the EU GDPR? – A Warning for U.S.-Only Businesses

By Thomas J. Smedinghoff and Elizabeth Kilburn

All U.S. businesses need to pay attention to the new and comprehensive EU-wide privacy law known as the General Data Protection Regulation¹ (GDPR), which takes effect on May 25, 2018. With its greatly expanded compliance obligations, tough penalty regime (fines can be as much as 4% of a company's worldwide gross revenue), and extra-territorial applicability, even businesses licensed to sell only in the U.S., and with no operations in the EU whatsoever, may nonetheless find that they are subject to the jurisdiction of GDPR.

Continuing to service customers who later moved to the EU, for example, may raise issues regarding whether a company's activities bring it within the jurisdiction of the GDPR, which is designed to protect the personal data of individuals in the EU, regardless of nationality.

The GDPR is a comprehensive reform of European data protection laws intended to strengthen online privacy rights and boost Europe's digital economy. It provides for a single set of rules for all organizations processing personal data from the EU, removing many of the inconsistencies across Member States that have been associated with the Data Protection Directive.

The extra-territorial scope of the GDPR is very broad, however, and will likely reach many U.S. businesses even though they do not have a presence in the EU. Generally, Article 3 provides that the GDPR will apply to U.S.-based companies in three cases:

If the U.S. Business has an "Establishment" in the EU

The GDPR applies to entities who are engaged in the processing of personal data *in the context of the activities of an establishment* in the EU, regardless of whether the processing takes place in the EU or not. However, establishment in the EU does not require the formal presence of a subsidiary or other legal entity.

The GDPR states that an establishment implies the *effective and real exercise of activity through stable arrangements*. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

¹ Available at <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679>

Prior interpretations of the term “establishment” under the Data Protection Directive make clear that that an establishment need not have a legal personality but that a stable establishment requires that “both human and technical resources necessary for the provision of particular services are *permanently available*.” Thus:

- Where ‘effective and real exercise of activity’ takes place, for example in an attorney’s office through ‘stable arrangements,’ the office would qualify as an establishment.
- A one-person office would qualify as long as the office does more than simply represent a controller established elsewhere, and is actively involved in the activities in the context of which the processing of personal data takes place.
- In any case, the form of the office is not decisive: even a simple agent may be considered as a relevant establishment if his presence in the EU presents sufficient stability.²

In one case, the European Court of Justice held that “the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question.”³

It is also important to note that processing personal data “in the context of” an establishment in the EU does not require processing by the EU establishment. The existence of an EU-based establishment may trigger applicability of the GDPR over a non-EU entity, even if that local EU establishment is not actually taking any role in the data processing itself, so long as there is an “*inextricable link*” between the activities of the EU establishment and the processing of data carried out by the non-EU controller.

For example, the European Court of Justice in the “Google Spain” case found that U.S.-based Google Inc. was processing personal data in the context of an EU establishment because its search activities were inextricably linked to the advertising sales generated by Google Spain, a local subsidiary established in the EU. Because the data processing at issue was related to the search business which Google Spain’s sale of online advertising helped finance, the court found that the processing by Google in the U.S. was carried out “in the context of the activities” of the Spanish establishment.

Therefore, if this “processing of personal data in the context of the activities of an EU establishment” test is met, the GDPR applies irrespective of whether the actual data processing takes place in the EU or not.

If the U.S. Business Offers Goods or Services in the EU

The GDPR also applies to businesses not established in the EU if they process the personal data of individuals who are in the EU when *offering them goods or services* (whether or not in return for payment). This applies to the processing of personal data of any “*data subjects who are in the Union*,” regardless of their nationality or residence – i.e., it covers the personal data of EU citizens, residents, tourists, and other persons temporarily in the EU (e.g., U.S. businesspersons or military personnel).

The question of what constitutes “offering” goods or services to EU residents is determined on a case-by-case basis. The only guidance on how to interpret this provision indicates that the focus for interpreting this requirement is on the *intention* of the non-EU entity, rather than on the *mere availability* of its goods or services.

² WP 179, Article 29 Working Party, Opinion 8/2010 on applicable law, December 16, 2010, at pp. 11-12.

³ *Weltimmo v NAIH* (Case C-230/14, October 1, 2015), at Para. 30.

Thus, while the mere availability of the website of a U.S.-based entity is not sufficient per se, the following website-related factors (among others) have been suggested as strong indications that a non-EU business is *intentionally* offering goods or services to data subjects in the EU and may therefore be subject to the GDPR:

- Use of the language of an EU Member State (if the language is different than the language of the business’ home state);⁴
- Use of the currency of an EU Member State (if the currency is different than the currency of the business’ home state);
- Use of a top-level domain name of an EU Member State;
- Mentions of customers based in an EU Member State; or
- Targeted advertising to consumers in an EU Member State.

A key question for businesses may well be the extent to which they offer goods or services to US-based customers who later move (either temporarily or permanently) to the EU, whether such services are offered through their website or other means.

If the U.S. Business Monitors the Behavior of Individuals in the EU

Businesses that are not established in the EU, and that do not offer goods or services in the EU, will nonetheless be subject to the GDPR if they process personal data *in connection with the “monitoring” of the behavior* of EU data subjects.⁵

The question of what constitutes “monitoring” is determined on a case-by-case basis, but analysis of the GDPR establishes that monitoring appears to be focused on internet activity that includes both:

- tracking an individual on the internet; and
- the use of data processing techniques to profile such individuals in order to analyze or predict personal preferences, behavior and attitudes.

The GDPR defines profiling to be any form of automated processing of personal data “to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict certain aspects concerning that natural person’s performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.”

Accordingly, it would seem that monitoring requires not only the gathering of personal data involving personal aspects of natural persons, but the automated processing of such data for the purpose of making decisions about the data subjects.

At this point, however, it is unclear exactly how detailed the monitoring of a data subject must be in order to trigger the application of the GDPR.

Any U.S. business which falls in to one of these three categories must start taking measures now to ensure it will be fully compliant by May 25, 2018.

⁴ See, e.g., the CJEU’s ruling in *Weltimmo* (Case C230/14), which emphasized that if a company operates a service in the native language of a country (in that case a Slovakian property advertising service operating in Hungary) it could be held accountable to that country’s data protection authority.

⁵ GDPR Article 3(2)(b) provides that: “This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: . . . (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.”

Incident Response – Privilege and Work Product Issues After *In re Premera*

By Brandon J. Montminy and Molly McGinnis Stine

Despite considerable incident response work after numerous alleged data breaches, very few opinions have addressed the application of attorney-client privilege and the work-product doctrine to the materials created by such work.

Recently, in *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, the United States District Court for the District of Oregon provided detailed analysis of the issues. The November 13, 2017 opinion concerned a class action brought against Premera after Premera's March 17, 2015 disclosure that its computer network had been breached. The Plaintiffs alleged that the breach compromised the confidential information of approximately 11 million current and former members, affiliated members, and employees of Premera. The Plaintiffs requested an order to compel Premera to produce certain documents, described by category, that Premera had withheld on assertions of attorney-client privilege or the work-product doctrine.

The four categories of materials sought by Plaintiffs' counsel were: (1) documents that Premera asserted incorporated the advice of counsel, but which were not prepared by or sent to counsel; (2) documents that Premera asserted were prepared at the request of counsel, but were not prepared by or sent to counsel and appear to be business documents not prepared because of litigation; (3) documents that relate to third-party vendor work on the data breach investigation and remediation; and (4) documents that Premera sent to third-parties. Premera asserts are subject to the joint defense or common interest exception to the waiver of privilege by disclosure. Although all four categories and the court's discussion of each are relevant and should be reviewed, this article focuses on the third category – the documents relating to the work done by Mandiant, a third party cybersecurity firm.

The court began by referring to the general law of attorney-client privilege and work-product doctrine applicable to all privilege disputes. Importantly, the court continued the reasoning of the United States District Court, C.D. California earlier this year, in applying the "because of" test to potential work-product materials prepared for dual purposes – litigation and any other – in the context of materials prepared following a data breach.

The third category of documents is of particular interest because it addresses, among others, documents relating to Mandiant's work for Premera. Mandiant was hired by Premera in October 2014 to review Premera's data management system. On January 29, 2015, Mandiant discovered the existence of malware in Premera's system. On February 20, 2015, Premera hired outside counsel in anticipation of litigation as a result of the breach. The next day, on February 21, 2015, Premera and Mandiant entered into an amended statement of work that shifted supervision of Mandiant's work to outside counsel. However, the amended statement of work did not otherwise change the scope of Mandiant's work from what was described in the Master Services Agreement between Mandiant and Premera entered into on October 10, 2014.

The court found that the amended statement of work did not support that Mandiant's focus shifted to an investigator working on behalf of outside counsel, and that the materials were not

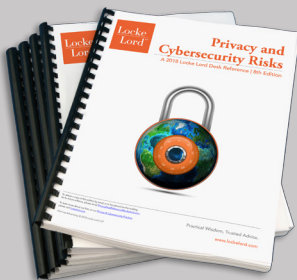
protected. In reaching its conclusion, the court differentiated two of the few relevant, prior cases. The first was *In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 WL 6777384 (D. Minn., Oct. 23, 2015). In that case, Target had dual-tracked the investigation and engaged separate teams: one to investigate the data breach generally, and the other to investigate through a company retained by counsel for the purpose of assisting the attorneys in providing legal advice and preparing for litigation. The *Premera* court described the distinction between the circumstances before it and those in *Target*:

With *Premera*, however, there was only one investigation, performed by Mandiant, which began at Premera's request. When the supervisory responsibility later shifted to outside counsel, the scope of the work performed did not change. Thus, the change of supervision, by itself, is not sufficient to render all of the later communications and underlying documents privileged or immune from discovery as work product.

Similarly, the court distinguished *In re Experian Data Breach Litigation*, 2017 WL 4325583 (C.D. Cal., May 18, 2017). In *Experian*, outside counsel was hired by the company and outside counsel then hired Mandiant. However, here, Premera had already hired Mandiant, which was performing an ongoing investigation under Premera's supervision before outside counsel became involved. The *Premera* court made it clear that Premera had the burden of showing that Mandiant changed the nature of its investigation, and failed to meet that burden.

This failure to sufficiently amend the statement of work was ultimately fatal to both assertions of attorney-client privilege as well as work-product protection. The *Premera* court did allow that Premera could properly withhold materials that were not "dual purpose," were prepared "for the purpose of communicating with an attorney" for legal advice, or did contain "the mental impressions of counsel prepared in anticipation of litigation."

This new decision and those before it collectively suggest some steps that an entity may want to consider to try to protect the work concerning its incident response. Each matter is different and the facts and applicable law of any given situation may affect whether attorney-client privilege and work product protection apply. While any entity should evaluate its own situation and consider discussing these issues with counsel, the following are among the possible topics about which to assess timing and relative merits: (1) identify and engage incident response counsel as soon as possible, working with one's insurer depending on the type of insurance coverage that may be involved, (2) have incident response counsel retain and direct the work of other third-party service providers, (3) have engagement letters appropriately indicate what work is being requested and for what purpose, including its role in assisting counsel in providing legal advice and in anticipation of litigation, (4) consider two parallel investigations as in *Target*, and (5) develop a strategy about with whom, internally and externally, incident response work is discussed and shared.



Locke Lord's Privacy & Cybersecurity Group will soon release the **8th edition Privacy and Cybersecurity Risks Desk Reference**. The Desk Reference discusses legal and regulatory privacy, data security and breach notification developments, legislative developments, exposures presented by data breaches, privacy issues arising out of new technologies, recent major breaches and court decisions, and lines of insurance potentially impacted. Click subscribe [HERE](#) to be notified of the release.



Practical Wisdom, Trusted Advice.

www.lockelord.com

Atlanta | Austin | Boston | Chicago | Cincinnati | Dallas | Hartford | Hong Kong | Houston | London | Los Angeles
Miami | Morristown | New Orleans | New York | Providence | San Francisco | Stamford | Washington DC | West Palm Beach

Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This brochure is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice. (122117)

Attorney Advertising © 2017 Locke Lord LLP