KING & SPALDING

Client Alert

Business Litigation Practice Group
Data, Privacy & Security Practice Group

July 19, 2016

First EU-wide cybersecurity regime set to enter force in August 2016 after final approval by European Parliament

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Jane E. Player
+44 20 7551 2130
jplayer@kslaw.com

Angela Hayes
+44 20 7551 2145
ahayes@kslaw.com

Kim Roberts
+44 20 7551 2133
kroberts@kslaw.com

Nicholas A. Oldham
+1 202 626 3740
noldham@kslaw.com

Bailey J. Langner
+1 415 318 1214
blangner@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

London
125 Old Broad Street
London, EC2N 1AR
Tel: +44 20 7551 7500

www.kslaw.com

Summary

The European Parliament gave final approval to the Network and Information Security Directive ("Directive"), the first-ever EU-wide cybersecurity standards, on July 6, 2016. The Directive seeks to improve the cybersecurity capabilities of member states, as well as improve cooperation on cybersecurity issues between EU nations. The new rules require "operators of essential services" and some internet services providers to adhere to minimum cybersecurity standards and report significant cyber-attacks to public authorities. The Directive puts an end to the fragmentation of individual cybersecurity systems currently in place in the twenty-eight member states, and substantially changes the cybersecurity regulatory landscape for many businesses that operate within the EU.

Data, Privacy & Security in the EU

The Directive is an outgrowth of the European Commission's 2013 Cybersecurity Strategy and proposed Directive on Network and Information Security. Although European authorities moved relatively quickly since reaching a provisional agreement on the new cybersecurity regime in December 2015, the law making process of the Directive took over three years.

Final approval of the Directive comes amidst a series of substantial changes to cybersecurity rules within Europe. The EU is well known for its stringent privacy laws, and developments over the past year reflect the EU's commitment to personal privacy protections. Just last week, EU member states voted in favor of the Privacy Shield, a new transatlantic data transfer agreement, and on July 12, 2016, the European Commission announced its approval and adoption of the Privacy Shield. The previous Safe Harbor agreement, invalidated by the Court of Justice of the European Union ("CJEU") in October 2015, had allowed US companies to self-certify that they would comply with more stringent EU data protection standards so as to allow for the free transfer of data from the EU to the United States. The CJEU found U.S. data security provisions insufficient, rendering Safe Harbor illegal.

In addition to the privacy of EU citizens, EU regulators are concerned about the financial costs associated with cybersecurity threats. The EU Agency for Network and Information Security ("ENISA") reported that security incidents result in annual losses that range from €260 to €340 billion. These figures include incidents caused by human error, technical failures, and malicious attacks. EU authorities often cite these figures to support the need for increasingly strict data privacy protections.

Network and Information Security Directive

The final iteration of the Directive parallels efforts throughout Europe to impose heightened security measures on companies that operate within the EU, both to improve data security and cut financial losses related to security incidents. The Directive, therefore, seeks to accomplish three related goals:

(i) Improve cybersecurity capabilities at a national level,

(ii) Increase cooperation on cybersecurity within the EU, and

(iii) Impose risk management and incident reporting obligations for "operators of essential services" and digital service providers.

Through a set of common rules and obligations, European authorities hope to achieve a high common level of network and information systems security across the EU. Though related and overlapping, the Directive imposes separate regimes for critical service sectors and technology firms, with each subject to differing standards and levels of scrutiny.

Improving Cybersecurity Capabilities

As a first requirement, member states must adopt the national Network and Information Security ("NIS") strategy, which defines and outlines the coordinated strategic objectives, appropriate policy, and regulatory measures related to cybersecurity within the EU. Member states must also designate at least one national competent authority to monitor the application of the Directive at the national level, as well as a single point of contact to ensure better cross-border cooperation between member nations. Moreover, each member nation will also be required to create one or more Computer Security Incident Response Team ("CSIRT") to monitor, respond to, and analyze incidents at a national level, as well as disseminate information to relevant stakeholders.

Cross-Border Security Incidents & Improving Cooperation

The Directive calls for the creation of two EU-wide groups to promote cooperation on cybersecurity matters. The Directive first establishes an EU-level strategic Cooperation Group to encourage member states to exchange information about breaches, as well as develop and share best practices for securing infrastructure. Representatives from member states and ENISA will comprise the Cooperation Group, and the European Commission will act as secretariat. The Cooperation Group will begin operating in February 2017, six months after the Directive enters into force.

Second, the Directive creates a network of the national CSIRTs. In addition to national responsibilities discussed above, CSIRTs will participate in the broader CSIRT Network so that EU nations may collectively address cross-border security incidents and oversee coordinated responses. In addition, the CSIRT Network is tasked with exchanging information on CSIRT services and information related to incidents, as well as issuing guidelines on operational cooperation. European authorities hope to increase trust and confidence between member states with the establishment of the CSIRT Network.

Obligations for "Operators of Essential Services"

The Directive applies to companies with a substantial impact on society and the economy, referred to as "operators of essential services." Such companies will be required to comply with new rules under the Directive. The Directive seeks to ensure that important infrastructure like airports, the water supply, and power stations are secure enough to resist online attacks. The Directive will cover operators in the following industries:

- *Energy*: Electricity, oil, gas
- *Transport*: Air, rail, water, road
- *Banking*: Credit institutions
- *Financial market infrastructures*: Trading venues, central counterparties
- *Health*: Healthcare settings
- *Water*: Drinking water supply and distribution
- *Digital infrastructure*: Internet exchange points, domain name system service providers, top-level domain name registries

However, not all companies within those industries will be subject to the Directive. Member states will be required to identify operators of essential services from covered sectors by assessing (by reference to set criteria in the Directive) whether the service is critical for society and the economy, whether the service depends on network and information systems, and whether an incident could have significant disruptive effects on its provision or public safety. Once identified, these critical service companies will be required to implement certain security measures to prevent cyber-attacks and minimize the impact of incidents on IT systems.

Critical service companies will also be required to report major security breaches. Rather than set out a specific set of rules and circumstances which require notification, the Directive defines three parameters that should be considered in determining whether a breach is significant: (1) the number of users affected, (2) the duration of the incident, and (3) its geographic reach. Acting together within the Cooperation Group, national competent authorities will further clarify reporting requirements in the future through the adoption of additional guidelines.

Digital Service Providers Under the Directive

Technology firms, or "digital service providers" ("DSPs"), will also be subject to an overlapping, but distinct, regime of rules under the Directive. Online marketplaces, as well as cloud computing services and search engines, will be subject to the new rules. Micro and small digital companies are exempt. DSPs, like operators of essential services, are required to comply with minimum security standards to prevent risks and minimize the effect of incidents on IT systems. The security measures for DSPs must also take into account additional factors such as business community management and compliance with international standards.

DSPs must also report significant data breaches to public authorities. Again, the Directive does not specify a threshold for whether an incident is "substantial" and requires notification to the relevant national authority. Instead, in the case of DSPs, it defines five parameters that should be taken into consideration: (1) the number of users affected, (2) the duration of the incident, (3) the incident's geographic reach, (4) the extent of the disruption to service, and (5) the impact on economic and societal activities. The European Commission, however, will adopt further guidelines on these parameters in the future by means of implementing acts.

Notably, member states are not permitted to impose additional, more stringent security or notification obligations on DSPs.

Next Steps

The Directive will soon be published in the *Official Journal of the European Union*, and the new regime will come into force twenty days after publication (August 2016). Member states will then have twenty-one months to implement the Directive and incorporate it into their national laws (May 2018), as well as six additional months to identify operators of essential services (November 2018). The European Commission will adopt additional implementing acts to clarify the security and notifications requirements of DSPs within a year of the Directive's adoption (August 2017).

Recommendations

The Network and Information Security Directive creates substantial compliance and regulatory obstacles to a broad range of businesses operating within the European Union. Companies subject to this Directive should examine their governance and compliance regimes, and work with outside counsel and experts in advance of a cyber incident. Understanding the Directive, its implementation procedure, which companies it will apply to, and the security and reporting obligations applicable to those companies, as well as monitoring future developments related to the Directive, will enable companies to successfully comply with the new requirements and prepare for the new EU cybersecurity landscape.

King & Spalding's Data, Privacy & Security Practice

With more than 60 Data, Privacy & Security lawyers in offices across the United States, Europe, and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and cybersecurity-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy. Our Data, Privacy & Security Practice has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

If you have any questions regarding the Network and Information Security Directive, related issues, or other changes to European privacy regulations referenced in this Client Alert, please contact Phyllis Sumner at +1 404 572 4799, Jane Player at +44 20 7551 2130, Angela Hayes at +44 20 7551 2145, Kim Roberts at +44 20 7551 2133, Nicholas Oldham at +1 202 626 3740, or Bailey Langner at +1 415 318 1214.

* * *