KING & SPALDING

Client Alert

Business Litigation Practice Group
Data, Privacy & Security Practice Group

December 17, 2015

European Parliament, Commission, and Council reach deal on draft text of Network and Information Security Directive, the first EU-wide cybersecurity regime

European authorities reached a provisional agreement on the Network and Information Security Directive, the first-ever EU-wide cybersecurity standards. Press releases from the **European Parliament**, **European Commission**, and **European Council** announced the December 7, 2015 deal. The Directive seeks to improve the cybersecurity capabilities of member states, as well as improve cooperation on cybersecurity issues between EU nations. Moreover, once formally approved, the new rules will require "operators of essential services" and some internet services providers to adhere to minimum cybersecurity standards and report significant cyber-attacks to public authorities. Notably, the Directive will put an end to the current fragmentation of individual cybersecurity systems by the twenty-eight member nations, and will substantially change the regulatory landscape for many businesses that operate within the European Union. This provisional agreement is an outgrowth of the European Commission's 2013 Cybersecurity Strategy and proposed Directive on Network and Information Security. More information about this earlier EU action can be found **here**.

Data, Privacy & Security in the EU

The Network and Information Security Directive comes amidst a flurry of substantial changes to cybersecurity rules and regulations within Europe. The European Union is particularly well known for its stringent privacy laws, and recent developments reflect a commitment to personal privacy protections. The European Court of Justice ("ECJ"), for example, invalidated the Safe Harbor framework on October 6, 2015. The Safe Harbor agreement 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 European data to the United States. According to the ECJ ruling, however, data stored on US servers does not meet EU standards, largely due to the US government's mass surveillance program—thus rendering the agreement illegal.

The privacy of EU citizens, however, is not the sole concern of European Union regulators. The EU agency for Network and Information Security ("ENISA") reports that security incidents are on the rise, resulting in annual

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

Alexander K. Haas
+1 202 626 5502
ahaas@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

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

www.kslaw.com

losses that range from €260 to €340 billion. These figures include incidents resulting from human error, technical failures, and malicious attacks.

Network and Information Security Directive

The current 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 losses related to security incidents. The Directive, therefore, seeks to accomplish three related goals:

(i) Improve cybersecurity capabilities in member states,

(ii) Improve cooperation on cybersecurity within the European Union, and

(iii) Require "operators of essential services" and key digital service providers to comply with specific security measures and report security incidents.

Through a set of common rules and obligations, EU authorities hope to strengthen network and information security across the EU. Though related, the Directive will create separate regimes for technology firms and critical service sectors, 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.

Cross-Border Security Incidents & Improving Cooperation

In addition to the national NIS strategy, the Directive calls for the creation of groups to promote cooperation on cybersecurity matters across Europe. The Directive will first establish 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. Moreover, each member nation will also be required to create a Computer Security Incident Response Team so that EU nations may collectively address cross-border security incidents and oversee coordinated responses. The establishment of these groups is consistent with the Directive's goal of increasing coordination within the EU, and European authorities hope to thereby increase trust and confidence between member states.

Security and Notification Obligations for "Operators of Essential Services"

Companies with a substantial impact on society and the economy, referred to as "operators of essential services," 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 certain operators in the following industries:

- *Energy*: Electricity, oil, gas
- *Transport*: Air, rail, water, road
- *Banking*: Credit institutions
- *Financial market infrastructure*: Trading venues, central counterparties

- *Health*: Healthcare providers
- *Water*: Drinking water supply and distribution
- *Digital infrastructure*: Internet exchange points, domain name system service providers, top-level domain name registries

Not all companies within those industries, however, will be subject to the Directive. Using set criteria, member states will identify operators of essential services from those sectors by assessing 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 report major security breaches, as well as implement certain security measures to resist cyber-attacks. Companies who do not comply will face sanctions.

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 like eBay and Amazon, as well as cloud computing services and search engines like Google, will be subject to the new rules. Although the specifics are still uncertain, these DSPs will likewise be required to comply with minimum security standards and report major data breaches to public authorities, or face sanctions. More importantly, the Directive will create a uniform regime of standards for digital service providers throughout the EU. The obligations affecting technology companies, however, are expected to be less stringent than the requirements that operators of essential services face. Moreover, small digital companies and social networks like Facebook will be exempt.

Next Steps

The draft text of the Directive will be presented to member states' ambassadors for approval on December 18, 2015. Thereafter, Parliament's Internal Market Committee and the Council Committee must still formally approve the provisional agreement. Once approved, the Directive will be published in the *Official Journal of the European Union*, and the new measures will enter into force. Member states will then have twenty-one months to implement the Directive and incorporate it into their national laws, as well as six additional months to identify operators of essential services.

Recommendations

The proposed Network and Information Security Directive will create substantial compliance and regulatory obstacles to a broad range of businesses operating within the European Union. Companies subject to this Directive should act accordingly and take care to examine their governance and compliance regimes and work with outside counsel and experts in advance of a cyber incident.

For those companies conducting business within the energy, transport, banking, financial market infrastructure, health, or water sectors, as well as technology firms operating search engines, online marketplaces, or cloud computing services, the Directive raises many unanswered questions. Understanding the Directive and its implementation procedure after the new measures are published, as well as monitoring future developments related to the Directive, will enable companies to successfully comply with new requirements and prepare for further changes.

King & Spalding's Data, Privacy & Security Practice

With more than 50 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, Alexander Haas at +1 202 626 5502, Nicholas Oldham at +1 202 626 3740, or Bailey Langner at +1 415 318 1214.