KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

January 5, 2016

For more information, contact:

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

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

Angela Hayes
+44 20 7551 21445
ahayes@kslaw.com

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

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

Kerianne Tobitsch
+1 212 556 2310
ktobitsch@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

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

www.kslaw.com

The European Union Reaches Agreement New Data Privacy and Security Standards

The EU Centralizes and Toughens Data Protection Rules

On December 15, 2015, European officials issued a **Press Release** announcing an agreement to enact common standards for data protection across all 28 member states to "put an end to the patchwork of data protection rules that currently exists."[1] The rules do not go into effect until the European Parliament and the national governments of the EU member states consider and formally adopt them in 2016, which is widely expected.[2] The rules would become effective two years after adoption. [3] The General Data Protection Regulation ("GDPR") and Data Protection Directive would codify the rules.[4]

Compared to the current Data Protection Directive 95/46/EC in effect since 1995 ("1995 Directive"),[5] the GDPR strengthens data protection in several notable ways, including, among other things: (i) applying privacy rules to entities based outside the EU; (ii) imposing large multi-million Euro administrative fines for violating a variety of EU data privacy requirements; (iii) codifying the "right to be forgotten," (iv) requiring notification of data breaches to regulators within 72 hours; (v) requiring notification to data subjects under certain circumstances; and (vi) requiring parental consent for children under the age of 16, including on social media sites.[6]

One of the most significant changes is to the organization of the regulatory structure.[7] The GDPR creates an overarching European Data Protection Board composed of a supervisory authority from each member state.[8] To reduce compliance costs for entities, the GDPR will only require entities to report to one lead supervisory authority,[9] which must coordinate and share information with any other concerned supervisory authorities.[10]

Another significant change is the prospect of increased regulatory enforcement and financial penalties. Specifically, the GDPR would allow supervisory authorities to issue large administrative fines of up to 4% of worldwide annual turnover for certain violations.[11] For large companies, including multinational companies operating in Europe, this could reach into the hundreds of millions of dollars.

Jurisdiction

The GDPR covers data controllers or processors that process personal data either wholly or partly by automated means, or by other means if the data is

part of a filing system.[12] It has greater reach than the 1995 Directive, which only applied to data controllers. Personal data is defined very broadly as any information relating to an identifiable person, such as name, identification number, location data, online identifier, or factors related to the physical, physiological, genetic, mental, economic, cultural, or social identity of a person.[13]

Importantly, the GDPR applies to the processing of personal data in the context of an entity's activities in the EU, "regardless of whether the processing takes place in the [EU] or not."[14] For example, this provision would apply to the processing of data through cloud services performed outside the EU.

According to the EC Press Release announcing the new Directive, the GDPR will apply a "European rules on European soil" model meaning that "companies based outside of Europe will have to apply the same rules [as European companies] when offering services in the EU." While the interpretation of the applicability of this provision may take time, the GDPR will apply to entities not established in the EU if data processing activities relate to the offering of goods or services in the EU, regardless of whether payment from the data subject is required, or relate to the monitoring of data subjects in the EU.[15] This provision is likely broad enough to encompass entities operating in a wide range of industries, including technology, finance, or consumer goods companies.

Processing and Consent

Similar to the 1995 Directive, the processing of personal data is lawful only if the data subject gives consent or if the processing is necessary to perform under a contract, comply with a legal obligation, protect the vital interests of a data subject, perform a task in the public interest, or carry out the legitimate interests of a data controller.[16] EU member states may enact more specific provisions.[17] Consent must be freely given, specific, informed, and unambiguous, and the data subject must consent by a statement or "clear affirmative action."[18] The consent obtained should also cover all processing activities carried out for the same purpose or purposes. [19] Data subjects must have the right to withdraw consent at any time.[20] Entities violating these provisions are subject to the penalty provisions set out below.

Rights of Data Subjects

The GDPR codifies the rights of data subjects, which include: (i) the right to receive information about the processing of personal data in a clear, concise, transparent, and accessible form; (ii) the right to receive information about the collection of data, including an explanation of the purposes and legal basis for the collection, the categories of data collected, whether an entity intends to transfer personal data to a third country, the length of time the entity will store the data, and the ability to request correction of data or lodge a complaint; (iii) the right to access one's own personal data; (iv) the right to request that an entity rectify inaccurate data; (v) the right to request erasure of data in certain circumstances, also known as the "right to be forgotten"; (vi) the right to place restrictions on an entity's processing of personal data; (vii) the right to receive data in a portable format; (viii) the right to object to certain processing, such as profiling or marketing, even if such processing is otherwise in the entity's legitimate interests; and (ix) the right not to be subject to decisions based solely on automated processing, such as profiling.[21]

Data Security

Entities must implement technical and organizational measures to secure personal data, including, as appropriate, (i) the pseudonymization and encryption of personal data, (ii) measures to ensure the confidentiality, integrity, and availability of data and the resilience of processing systems, (iii) the ability restore the availability of and access to data in a timely manner, and (iv) a process for regularly testing, assessing, and evaluating the effectiveness of these security measures.[22] The appropriate level of security depends on the risks presented by an entity's data processing, such as the risk of unauthorized disclosure of or access to personal data.[23] Entities may use an approved code of conduct or certification mechanism to demonstrate compliance with these security requirements. [24]

In the event of a breach involving personal data, entities must notify the supervisory authority within 72 hours after discovery, unless the breach is "unlikely to result in a risk for the rights and freedoms of individuals."[25] The timing component makes this requirement far more stringent than notification obligations in the United States. Furthermore, entities must notify data subjects of a breach involving personal data that "is likely to result in a high risk [to] the[ir] rights and freedoms," unless the entity implemented appropriate security measures, such as encryption, or notification would involve a disproportionate effort by the entity.[26] This is a departure from the EU's current approach, which is inconsistent across member states but generally does not require consumer notification outside of certain industry sectors.

Another notable rule is that entities must conduct a privacy impact assessment when processing data with new technologies likely to result in high risk to the rights and freedoms of data subjects, and must consult with the supervisory authority in the absence of mitigation measures.[27] This provision may raise the cost for entities seeking to tweak their processing practices and force entities to consider the potential risk to data before making changes.

Transfers of Data

Entities may only transfer personal data to a third country if that country ensures an adequate level of protection.[28] Even if the third country as a whole does not provide an adequate level of protection, the GDPR departs from current law by permitting transfers to certain sectors within the third country that the EC specifies as providing an adequate level of protection.[29] Binding Corporate Rules (BCRs) and Model Clauses are still available as appropriate safeguards for the transfer of data.[30] Violations related to the transfer of personal data are subject to administrative fines described below.[31]

Penalties

Every data subject has the right to lodge a complaint with the supervisory authority[32] or to seek an effective judicial remedy against legally binding decisions of a supervisory authority before the courts of the member states.[33] Supervisory authorities may impose administrative fines ranging from up to 10,000,000 EUR or 2% of worldwide annual turnover (for lesser violations) to the greater of 20,000,000 EUR or 4% of *worldwide* annual turnover for violations involving the legal basis for data processing or transfer of personal data.[34] The GDPR lists factors, such as the nature, gravity, and duration of the infringement, steps taken to mitigate damage, and adherence to approved codes of conduct or certification mechanisms.[35] Obviously for large multi-national corporations, this penalty has the potential to reach hundreds of millions, if not billions, of dollars.

Takeaways

While the new EU rules on common standards for data protection are a welcome step towards a unified set of data protection rules in Europe, in the short and intermediate term, it is likely that member states may continue to adopt piecemeal approaches to data protection. The rules and reforms above are not immediately applicable. Rather the European Parliament and member states must consider and formally adopt them and the new rules will become applicable two years thereafter.

There remain open questions surrounding the interpretation and scope of the new data protection rules. For example, there is uncertainty about what type of breach would result in "risk for the rights and freedoms of individuals" and trigger the notification obligations to regulators or data subjects. It is also unclear what type of "clear affirmative action" constitutes consent as a legal basis for the processing of personal data. Do data subjects consent by accepting terms and conditions on a web page? Do they need to consent every time they conduct a transaction or is once sufficient? Since violation of the consent requirement is one of the triggers for the largest administrative fines, answers to these questions will be important.

While one of the stated goals of this reform is to "creat[e] [] business opportunities" by reducing "burdensome" rules and the cost of compliance,[36] entities still should expect to face significant compliance costs in the short term. On the one hand, the new rules try to reduce the burden on entities by eliminating the burden of coordinating with multiple supervisory authorities and permitting entities to tailor security measures based on risk. But entities should still be prepared to face costs navigating the new European Data Protection Board and revising internal policies and procedures to account for the more stringent privacy rules required by the GDPR.

In light of these open questions and the potential for significant new regulatory burdens and substantial fines under the new EU rules, companies should proactively examine their data collection, retention, and use policies, particularly as they pertain to information about individuals. Companies will need to develop or revise their governance programs to ensure effective and forward-looking compliance with these rules and ensure that they can protect themselves in the regulatory actions and inquiries that are likely to arise.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

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 data security-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.

---

[1] Press Release of European Commission, "Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market" (Dec. 15, 2015), *available at* http://europa.eu/rapid/press-release_IP-15-6321_en.htm [hereinafter "EC Press Release"].
[2] EC Press Release.
[3] EC Press Release.
[4] EC Press Release.
[5] Data Protection Directive 95/46/EC, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
[6] Draft General Data Protection Regulation, Regulation No. XXX/2016 of the European Parliament and of the Council [hereinafter "Draft GDPR"], *available at* https://iapp.org/media/pdf/resource_center/2015_12_15-GDPR_final_outcome_trilogue_consolidated_text.pdf. When the GDPR is formally adopted, the numbering of provisions is subject to change.
[7] EC Press Release.

[8] Draft GDPR, at Article 64.
[9] EC Press Release.
[10] Draft GDPR, at Articles 54a-56.
[11] Draft GDPR, at Article 79.
[12] Draft GDPR, at Articles 2-3.
[13] Draft GDPR, at Article 4.
[14] Draft GDPR, at Article 3.
[15] Draft GDPR, at Article 3.
[16] Draft GDPR, at Article 6.
[17] Draft GDPR, at Article 6.
[18] Draft GDPR, at Article 4(8).
[19] *See* Draft GDPR, at Article 6.
[20] Draft GDPR, at Article 7.
[21] Draft GDPR, at Articles 12-20.
[22] Draft GDPR, at Article 30.
[23] Draft GDPR, at Article 30.
[24] Draft GDPR, at Articles 22, 30, 38-39.
[25] Draft GDPR, at Article 31.
[26] Draft GDPR, at Article 32.
[27] Draft GDPR, at Articles 33-34.
[28] Draft GDPR, at Article 41.
[29] Draft GDPR, at Article 41.
[30] Draft GDPR, at Article 42.
[31] Draft GDPR, at Article 79.
[32] Draft GDPR, at Article 73.
[33] Draft GDPR, at Article 74.
[34] Draft GDPR, at Article 79.
[35] Draft GDPR, at Article 79.
[36] EC Press Release.