HUNTON& WILLIAMS

Client Alert

April 2016

EU General Data Protection Regulation Finally Adopted

On April 14, 2016, after four years of drafting and negotiations, the long awaited EU General Data Protection Regulation ("GDPR") has been adopted at the EU level. Following today's vote in plenary session by the EU Parliament, the GDPR is now officially EU law and will directly apply in all EU countries, replacing EU and national data protection legislation. Companies will be given a two-year transition period from the day the GDPR is published in the Official Journal of the EU in the next couple of weeks. The GDPR forms a new data protection landscape in Europe with stricter requirements and higher fines for the foreseeable future. It is expected to be highly influential in other regions of the world, affecting the way global businesses operate. The GDPR will become effective in Spring 2018. Businesses should use this time to review their existing practices, conduct gap analyses and start preparing for GDPR implementation.

The New Data Protection Landscape in Europe

The following is a summary of the key aspects of the GDPR that are relevant for businesses:

- **Broader scope:** The GDPR will apply to data processing activities of a data controller or a data processor established in the EU. In addition, it will apply to data controllers and data processors established outside the EU where their processing activities relate to the offering of goods and services to individuals in the EU or to the monitoring of EU individuals' behavior. This means that the GDPR will apply virtually to all businesses serving or targeting individuals in the EU market.

- **Concept of personal data:** Under the GDPR, location data, IP addresses and online identifiers would constitute personal data in most cases as this data could be used to identify individuals, in particular when combined with unique identifiers. Pseudonymization of personal data is considered a security measure used to limit the risk of singling out an individual during the processing. In addition, genetic data and biometric data are recognized as sensitive data requiring extra protection.

- **Data controllers, processors, joint controllers:** The GDPR will introduce additional obligations for data controllers, data processors and joint controllers. Direct obligations will be imposed on data processors for the security of personal data. Data processors can also be fined directly for non-compliance with the GDPR. Data processing agreements should have a specific minimum on content and conditions for further processing will be strengthened. Joint controllers will have to allocate responsibilities between them by contract or similar arrangement. Irrespective of the terms of such arrangement, individuals will be able to exercise their rights against each controllers.

- **Accountability obligations:** Companies will have to implement appropriate privacy policies and robust security measures, perform data protection impact assessments in certain cases and appoint a data protection officer under specific conditions. In addition, both data controllers and data processors will have to maintain records of data processing activities, replacing the existing registration and authorization obligations with the supervisory authorities.

- **Data breach notification:** The GDPR introduces a general data breach notification requirement that will apply across all industry sectors and will require data controllers to notify the competent supervisory authority within 72 hours after becoming aware of a data breach, unless they can provide a reasoned justification for the delay. If the breach is likely to result in a high risk for the individuals' rights and freedoms, data controllers will also have the obligation to notify individuals of the breach without undue delay.

- **One-stop shop:** For companies active in multiple EU countries, the GDPR will allow them to have a central point of enforcement through the one-stop shop mechanism. The supervisory authority of the main establishment or of the single establishment of the data controller or data processor in the EU will act as the lead supervisory authority, supervising all their processing activities throughout the EU. This new mechanism will allow data controllers and data processors to interact with a single lead data protection authority ("DPA"); however, other DPAs may have a say for cross-border operations as the GDPR includes significant consistency and cooperation procedures. In addition, each individual supervisory authority will be competent to handle purely local complaints or deal with purely local infringements of the GDPR.

- **Consent:** Consent should be a freely given, specific, informed and unambiguous indication of the individual's wish to, either by a statement or by a clear affirmative action, agree to the processing of his or her personal data. The GDPR puts emphasis on the fact that the processing should not be made conditional on the individual's consent. The GDPR also provides specific protection in the context of children's personal data by strengthening the validity conditions of children's consent. When offering information society services directly to children under the age of 16 – or a lower age provided by EU Member State law which may not be below 13 years – consent should be given or authorized by the holder of parental responsibility.

- **Profiling:** The GDPR will strengthen the protection of individuals against possible negative effects of profiling by providing them with the right not to be subject to automated decision making (including profiling), which produces legal effects concerning the individual or significantly affects the individual. Furthermore, profiling involving solely sensitive personal data is prohibited unless carried out with the explicit consent of individuals, or if the profiling is necessary for reasons of substantial public interest. Stricter information obligations when performing profiling also will apply.

- **Privacy notices:** Under the GDPR, data controllers must take appropriate measures to provide individuals with information regarding the processing of their personal data. Information will have to be provided in a concise, transparent, intelligible and easily accessible form. The GDPR also introduces the use of standardized icons as a valid way to inform individuals.

- **Data transfers:** The GDPR maintains the general prohibition of data transfers to countries outside the EU that do not provide an adequate level of data protection. Consistent with the *Schrems* decision of the Court of Justice of the European Union, stricter conditions will apply for obtaining an "adequate" status. EU Model Clauses will remain a valid mechanism to transfer personal data outside the EU. Further, the GDPR explicitly recognizes and promotes the use of Binding Corporate Rules as a valid data transfer mechanism. Approved codes of conduct also can be used for data transfers.

- **Rights of individuals:** The GDPR will expand the rights of individuals. The GDPR reinforces the existing right to request the erasure of personal data that is no longer necessary by including a "right to be forgotten." It also introduces a right to data portability allowing individuals to transit and move personal data concerning them between providers.

- **Administrative fines:** Supervisory authorities will be given significantly more power to enforce compliance with the GDPR, including investigative, corrective, advisory and authorization powers.

In addition, supervisory authorities will have the power to impose administrative fines of up to a maximum of €20 million or 4 percent of the data controller's or data processor's total worldwide global turnover of the preceding financial year, whichever is higher.

- **Leeway for EU Commission acts:** The European Commission will have the power to adopt implementing and delegated acts that supplement some requirements of the GDPR, such as the information to be presented by icons, the procedures for providing standardized icons, or the format and procedures for mutual assistance between supervisory authorities.

- **Leeway for national law:** Under the GDPR, EU Member States will have a certain margin to introduce laws setting out specific conditions for the application of the GDPR, such as providing authorization of automated processing of personal data under certain conditions, setting out the age of children for required parental consent, or specifying the safeguards for processing of sensitive personal data in certain cases.

- **Human Resources data:** Under the GDPR, EU Member States may, by law or collective agreements, provide specific rules regarding the processing of employees' personal data in the employment context.

Conclusion

The GDPR will apply to all businesses in and outside Europe that deal with personal data of EU individuals. Businesses should take advantage of the two-year transition period to prepare for a significant increase in their data protection responsibilities and advance their privacy compliance programs. Undoubtedly, the GDPR aims to create a more mature and robust data protection landscape in Europe, which will help build data protection in businesses' every day programs.

Hunton & Williams' Global Privacy and Cybersecurity Practice

Hunton & Williams' award-winning global privacy and cybersecurity practice focuses on all aspects of privacy, data protection, cybersecurity, information governance and e-commerce issues for multinational companies across a broad range of industry sectors. In Europe, the practice extends beyond legal advice to integrated consulting on corporate privacy risk management, as well as legislative and strategic policy advice, business consulting on corporate information policy, and legal compliance. Our lawyers also recently released "The EU General Data Protection Regulation, a Guide for In-House Lawyers," which is available at www.huntonprivacyblog.com.

Contacts

Wim Nauwelaerts
wnauwelaerts@hunton.com

Lisa J. Sotto
lsotto@hunton.com

Bridget Treacy
btreacy@hunton.com

Aaron P. Simpson
asimpson@hunton.com