PAUL ELLIS LAW GROUP
OUR PRACTICE. YOUR SUCCESS.

CLIENT ALERT

April 2018

Are You Ready For the GDPR?

The EU General Data Protection Regulation (GDPR) goes into effect on May 25, 2018. When it does, it will usher in a new era that changes the data privacy landscape for millions of companies in Europe and around the world. For those that have yet to ensure that they are in full compliance, this alert contains critical information regarding who will be impacted by the GDPR and how they should prepare their business for the new regulatory regime.

The GDPR is designed to significantly increase the protections around the personal data of European citizens, and harmonizes all of the data privacy requirements across the European Union (EU). If your business provides products or services to EU citizens and collects, processes or stores any of their personal data – whether you do it directly yourself or outsource it to a business partner or contract service provider – you will be subject to the GDPR and must comply with its requirements.

The Paul Ellis Law Group stands ready to actively engage with clients to help them meet the approaching GDPR compliance deadline. We can provide you with practical solutions to help accelerate your efforts to prepare for the new data privacy regulations.

GDPR FUNDAMENTALS

What types of data does the GDPR protect?

The personal data of EU citizens, including:

- Identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation data

Who is required to comply with the GDPR?

Any company that collects, stores or processes the personal data of EU citizens must comply with the GDPR, even if the company does not have a business presence within the EU.

How does the GDPR affect my company's policies and business contracts?

The GDPR emphasizes accountability and well-documented compliance procedures. To comply, companies should maintain compliance policies, internal assessment reports, legal contracts and other documentation. The GDPR places equal liability on data controllers (the organizations that own the data) and data processors (the organizations that help manage that data). Your organization may be one, or the other, or both. If you are a data controller and your data processor is not in compliance, that means your organization is not in compliance. The GDPR also has 72-hour reporting requirements for breaches that everyone in the chain must be able to comply with. Companies must also inform customers of their rights under the GDPR.

This means that all existing contracts with processors (e.g., cloud providers, SaaS vendors, or payroll service providers) and customers may need to be revised to spell out data management responsibilities, and new contracts may need to be negotiated. Ultimately, all contracts involving the personal data of any EU citizen will need to define consistent processes as to the way in which data is managed and protected and breaches are reported.

What happens if my company is not in compliance with the GDPR?

The GDPR provides for significant penalties – up to €20 million or 4 percent of global annual turnover, whichever is higher – for non-compliance.

PREPARING FOR THE GDPR

What should my company be doing to prepare for the GDPR?

- **Conduct a risk assessment –** Your company should determine how it stores and processes data on EU citizens and understand the risks surrounding it. The risk assessment should also outline measures taken to mitigate that risk, including possibly re-evaluating and replacing prior practices relating to data flows and data transfers. This is particularly true for business relying on monitoring activities, such as online advertising.

- **Implement measures to mitigate risk** – Once you have identified the risks and how to mitigate them, you must put those measures into place. For many companies, that means revising existing risk mitigation measures.

- **Embrace privacy by design** – Ensure that privacy measures are incorporated into any new processing or product that is adopted. This should be thought about early in the process, if possible, to enable a structured assessment and systematic validation.

- **Set up a process for ongoing assessment** – Adopt a proactive approach to compliance by establishing a culture of monitoring, reviewing and assessing your data processing procedures. Aim to minimize data processing and retention of data and build in safeguards. Auditable privacy impact assessments will also need to be conducted to review any risky processing activities and steps taken to address specific concerns.

- **Prepare for data security breaches** – Put in place clear policies and procedures to ensure that you can detect and react quickly to a data breach and provide timely notifications, where required.

- **Establish a framework for accountability** – Ensure that you have clear policies in place, including both internal and customer-facing policies, to prove that you meet the required standards. Check that your team is trained to understand their obligations. If required, appoint a data protection officer.

- **Consider whether you have new obligations as a processor** – Understand your direct obligations as a processor under the GDPR and build applicable compliance measures into your policies, procedures and contracts. Consider whether your contracts are adequate and, for existing contracts, determine who bears the cost of making changes to the services as a result of the changes in laws or regulations. If you obtain data processing services from a third party, it is very important to determine and document your respective responsibilities.

How can the Paul Ellis Law Group help your company?

There are a number of ways in which we can help you and your company to prepare for the GDPR. Our attorneys can work with you to assess your existing internal data privacy policies and procedures and develop new or additional policies to facilitate compliance. We can review your business relationships and practices with your outside data controllers and data processors to ensure that you have documentation in place that addresses each party's legal obligations regarding the protection and handling of personal data. We can help you to understand the sources of your exposure and risk, develop a risk management strategy and help you address compliance issues, including data breaches, if they arise.

For more information about the GDPR, or for assistance in getting your company GDPR-ready, contact your primary contact at our firm or Paul Ellis at pellis@pelglaw.com/212-949-5900 x301.

This Client Alert is for informational purposes only, and is not intended to be legal advice.