General Data Protection Regulation

GUIDELINES FOR COMPANIES

The European Union's ("EU") General Data Protection Regulation ("GDPR") went into effect on May 25, 2018. The new privacy protocols have a far greater reach than prior EU Privacy regulations, and have been applied by certain global companies to American-based businesses even if these businesses do not have offices or employees in the EU. Penalties for non-compliance with GDPR can reach up to 4% of a violating company's worldwide revenue.

To assess if your company needs to comply with the GDPR, please consider the following questions:

1. Does your company have a branch, office, subsidiary or other establishment in the EU that collects, receives, transmits, uses, stores or otherwise processes personal data?
2. Does your company target goods or services to individuals residing in the EU?
3. Does your company develop user profiles or otherwise track the online activity of any individuals in the EU?

If any of the answers to these questions is yes, then it is likely your company should take actions to comply with the GDPR.

The **first step** should be appointing a Data Protection Officer, who will be responsible for responding to customer issues relating to privacy and responding to potential customers regarding GDPR compliance.

As a **second step**, the company should address the following questions:

- What customer/client data does the company obtain?
- How long is such data stored?
- How does the company use the data?
- Is this use justified to achieve the company's commercial purpose?
- Is the length of time the data is stored necessary for the company to achieve that purpose, or can it be shortened?
- Is there any information the company collects about customers or individuals that they may not be aware of?

As a **third step**, the company should implement the following:

- privacy policy,
- consent notices,
- client authorizations, and
- any notifications/documentation the company provides to customers or which it requires them to sign when providing information to the company.

Once the above has been compiled, compliance with the GDPR begins with ensuring that all information is collected transparently with the knowing consent of the individual from whom it is obtained. Thereafter, customers have the right to see their personal information and the right to request that that personal information be deleted from the company's servers.

Niles, Barton & Wilmer, LP can assist with this three-step process and revise a company's privacy policy, notifications, and processes, as necessary, to ensure compliance with the GDPR. We also advise updating vendor and affiliate agreements to ensure they indemnify the company for the vendor/affiliates GDPR violations. This is especially important for EU affiliates or partners.

Should you have any specific questions about your company's compliance with the GDPR, please do not hesitate to contact the members of Niles, Barton & Wilmer's Data Privacy and GDPR Practice Group:

Michael P. Shaw, Esquire
Partner
(410) 783-6382
mpshaw@nilesbarton.com

Matthew J. Youssef, Esquire
Associate
(410) 783-6357
mjyoussef@nilesbarton.com

GDPR GENERAL COMPLIANCE CHECKLIST

- ☐ Appoint a Data Protection Officer
- ☐ Ensure personal data of customers is identified as confidential and obligate personnel and third party vendors to adhere to similar confidentiality obligations
- ☐ Implement a process to notify Data Protection Officer of a data breach incident as soon as it becomes known, and provide support
- ☐ Only process personal data to the extent authorized in writing by the Data Protection Officer
- ☐ Ensure Company has the technical capacity to delete all of a customer's personal data when so requested by customer
- ☐ Ensure that GDPR-approved safeguards are in place before transferring customer personal data across borders (or confirm that the "receiving" country is on the EU Commission's list of approved countries)
- ☐ Train all employees annually on IT security and privacy compliance, and new employees as they are hired.
- ☐ Update the company's online privacy policy and review it annually.
- ☐ Update the company's written information security policy and review it annually.