42. **Keene Village Plastics**
46. **Premio Inc.**

GDPR FOCUS

HOW THE EUROPEAN UNION'S NEW CYBERSECURITY MEASURE WILL IMPACT YOUR AMERICAN MANUFACTURING BUSINESS. *BY DAN MESSELOFF AND EMILY KNIGHT*

As concerns about cybersecurity and data privacy weigh more and more heavily on the minds of corporate executives in manufacturing companies around the United States, the European Union has initiated expansive new efforts to protect its citizens from cybersecurity risks.

The EU's initiative – the General Data Protection Regulation (GDPR) – is far broader than any cybersecurity measure ever seen before in either the European Union or in the United States. More importantly, as a result of the reach of the GDPR, millions of American companies may unknowingly be at risk of violating the new law. The good news is there are measures you can take to comply with the GDPR.

I. What exactly is the GDPR?

On May 25, 2018, the GDPR will go into effect. The GDPR grants EU supervisory authorities the power to investigate compliance with the GDPR, issue warnings and impose administrative fines on entities that violate the GDPR. Additionally, individuals whose information may have been compromised as a result of any such violations may lodge complaints with supervisory authorities for violation of the GDPR. What makes the GDPR so fearsome is that the law authorizes fines of up to € 20 million (approx. $25 million) or 4 percent of a company's global revenue, whichever is greater.

At the most basic level, any company in the world that "processes" (including collecting and/or storing) the personal data of any individual in the EU will be subject to the GDPR's requirements, and therefore potentially subject to the GDPR's penalties. The GDPR broadly defines the term "Personal Data," and thereby increases the number of entities that will be considered "processors" of such data. The GDPR also creates a whole new set of rights for EU citizens whose personal data is being processed or handled, as well as a whole new set of requirements for entities subject to the law.

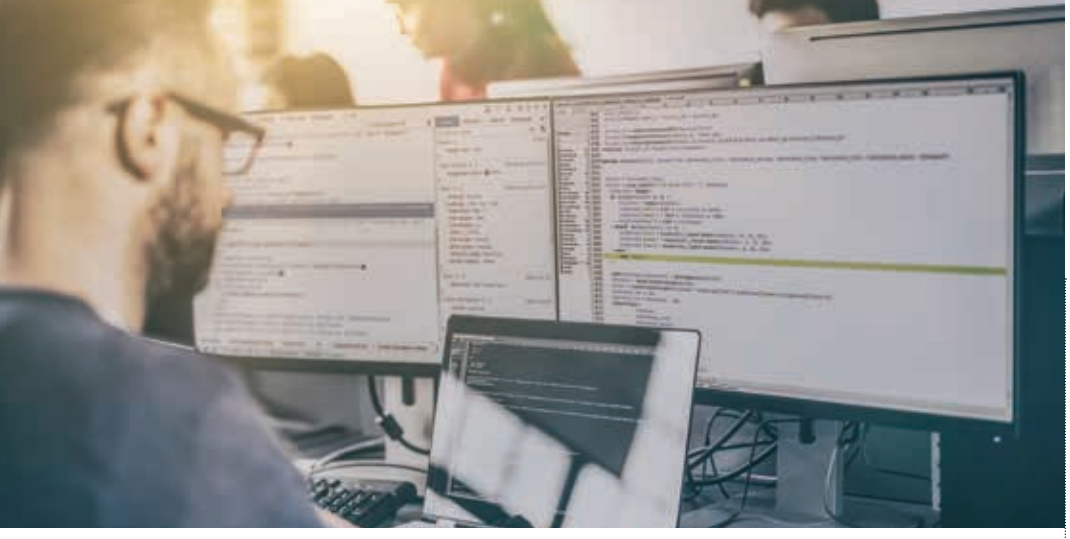
There are two primary ways a non-EU entity can become subject to the GDPR:

- **Entities Offering Goods or Services in the EU** – Companies that offer goods or services in the EU and handle personal identifiers (such as acceptance of payment by credit cards and e-mail addresses obtained for order confirmations) are subject to the GDPR. For example, a company whose website is merely accessible by EU residents would not bring the company within the jurisdiction of the GDPR, but if the website offers content in the language of the EU resident, accepts Euros or other European currency for payment, or otherwise appears to be targeting EU residents as customers, this would render the company subject to the GDPR.
- **Entities with EU "Establishments"** – Establishments are subject to the GDPR, although the definition of "establishment" is not clear. The GDPR explains that a company's activities, conducted "through stable arrangements" is sufficient for a finding of an establishment under the GDPR. For instance, if a U.S. company has an EU subsidiary that handles personal identifiers, that U.S. company is likely an establishment subject to the GDPR. Likewise, having even a single sales representative based in and tasked with selling products in the EU will likely be sufficient to constitute an establishment. On the other hand, merely maintaining a computer server in the EU may not satisfy the definition of "establishment" under the GDPR.

The GDPR broadens the scope of what constitutes personal data, defining it as any of the "information relating to an identified or individual person." Personal Data includes obvious identifiers, such as an individual's name, photos, email address, bank details and medical information; however, many less-known identifiers, such as login information, VINs, social media posts and network addresses, also now fall under the GDPR's new definition of personal data.

II. What is required?

Most U.S. entities will become subject to the GDPR by virtue of soliciting and collecting the information of customers in the EU. »



» U.S. companies that are subject to the GDPR should take immediate steps to make sure they will comply with the new law. While the GDPR sets forth a long and complex list of requirements, a few simple actions can go a long way in ensuring GDPR compliance.

1. Review your data retention.
Manufacturing companies and all other entities should begin reviewing their data retention policies. Although recent high-profile data breaches have caused many companies to improve their data retention policies, the GDPR includes requirements that may be more intensive than current best practices. For example, the GDPR's requirement that data must be stored for a limited amount of time and be deleted once it is no longer needed is burdensome, costly and completely new to U.S. companies. As such, companies should review and understand exactly what they are retaining and what they are destroying, as well as when and why they are doing so.

2. Be aware of personal data.
The GDPR's definition of personal data greatly expands the universe of data that is considered personal information and should give even the most vigilant data hawks cause for concern. For instance, the GDPR suggests that website "cookies," the small bits of information that are collected and stored to preserve website users' log-in information, is personal data. All U.S. companies that may be subject to the GDPR should take a long look at the information they are gathering and seriously review whether they are already collecting personal data from data subjects in the EU.

3. Be more prepared.
The GDPR's new 72-hour breach notification rule has already proven to be one of the most concerning aspects of the GDPR. The GDPR greatly reduces the amount of time that U.S. companies will have to respond to a data breach that affects data subjects, and it is not clear if it is even feasible to isolate, understand and provide authorities a notification of a data breach within 72 hours.

4. Revise your privacy policies.
U.S. companies should consider how the GDPR's scope and consent requirements affect how companies interface with consumers, including:

- Personal data – The broadening scope of personal data means more individuals will become data subjects, which in turn means that U.S. companies must undertake an increased burden to obtain consent to use their information.
- Consent to collect personal data – The GDPR's consent requirements will prove to be yet another significant burden for U.S. companies. The GDPR requires entities to make a clear request to collect personal data and requires data subjects to clearly affirm their consent.
- Data subjects' control over personal data – U.S. companies that are subject to the GDPR will need to stay vigilant to ensure that data subjects' requests are received and satisfied. On a practical level, U.S. companies will need to make sure that an individual who can field and respond to data subjects' requests is in place.

5. Look at third-party vendors.
The GDPR will make U.S. companies more accountable to their third-party data handlers. The GDPR's system of self-policing between data collectors and data handlers is analogous to the "business associate" requirements found in the Health Insurance Portability and Accountability Act (HIPAA), so many U.S. companies may already be prepared to ensure that their third-party vendors are in compliance with the GDPR. However, it will still be necessary to review all third-party vendors your company deals with because the scope of personal data under GDPR is much broader than "protected health information" under HIPAA.

6. Educate upper management.
Many executives and directors mistakenly believe data protection requires a sort of advanced skillset; however, the first steps to satisfying the duty of care with data security are well within a management team's capabilities. Given the recent attention to and increased understanding of the harmful effects of data breaches, directors now almost certainly have a duty to ensure that their companies are prioritizing data security. In this respect, the GDPR presents an opportunity to review your company's data security policies and procedures.

7. Review your existing cybersecurity and data privacy policies (and add some new ones).
Most U.S. companies recognize the

increased scrutiny of their cybersecurity and data privacy policies, and many have already taken steps to improve such policies. GDPR or not, every company that deals with individuals' data should have data security policies and procedures in place. If your company does not currently have data security policies and procedures, you should take immediate steps. If your company already has data security policies and procedures, it is time to review them to ensure compliance with the GDPR and that they reflect the realities of the current data security climate.

8. Audit your data security procedures.

In addition to reviewing your company's policies, you should consider conducting a data security audit. Such audits typically include a review component, including investigating how your company obtains, uses and maintains personal data, and a review of contracts with third-party vendors to establish a good-faith effort to ensure that your vendors are properly handling individuals' personal information. Audits also may include a preparedness component, where key executives and employees of the company meet and review the company's data breach policies and then practice data breach scenarios, including how to properly respond to a data breach and how to provide adequate notice to the proper authorities.

9. Think about your customers.

Of all the GDPR rules, the requirement to obtain consent to collect data is probably the most unique and difficult to address. To make matters worse, while the GDPR creates the arduous requirement of obtaining consent, the law is short on just how a company can obtain such consent. U.S. companies should begin considering the method they will use to obtain consent from customers in the EU to collect their information. Crafting proper consent procedures will likely be time consuming, so companies should not delay in considering how to comply with the new law.

When the GDPR goes into effect in May 2018, it will be a whole new world for thousands of companies and millions of individuals in the United States and the EU. With these tips, hopefully your manufacturing company will be prepared for it. **mt**

Dan Messeloff is a partner in the Privacy and Data Security practice group at Tucker Ellis LLP and oversees the firm's GDPR compliance team. He is also an active member of the firm's Labor & Employment and Business Litigation practice groups. He can be reached at 216.696.5898 or daniel.messeloff@tuckerellis.com.
Emily Knight is an associate in the Trial Department at Tucker Ellis LLP. She can be reached at 216.696.4893 or emily.knight@tuckerellis.com.