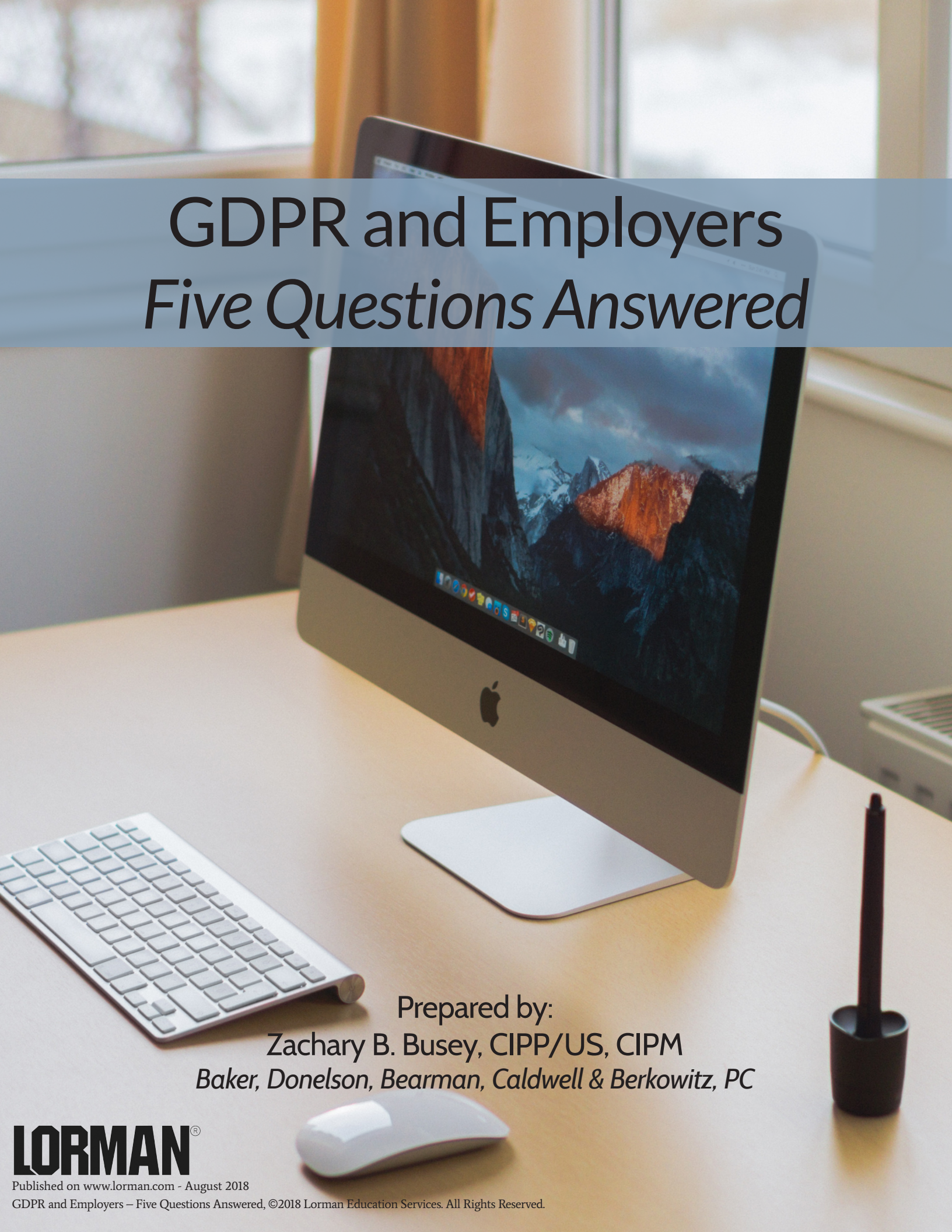

GDPR and Employers
Five Questions Answered

Prepared by:
Zachary B. Busey, CIPP/US, CIPM
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

LORMAN®

Published on www.lorman.com - August 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

GDPR and Employers – Five Questions Answered

Written by Zachary B. Busey, CIPP/US, CIPM – 5/30/18

The European Union's General Data Protection Regulation (GDPR) is a far-reaching and formidable regulatory scheme that governs the processing and handling of personal data. Although it formally took effect on May 25, 2018, employers may still be working to understand how GDPR affects their operations. We covered many of these issues extensively in a previous article, and we now turn to the top five questions employers are asking.

We only operate in the U.S. GDPR has no impact on our HR and employment practices, right?

Not necessarily. First and foremost, in this article, we are talking only about HR and employment practices. For answers on whether a company's business practices or broader operations trigger GDPR, check out our three-part webinar series on general coverage issues.

From an employment standpoint, there are two situations that will generally trigger GDPR: (1) when HR functions are based in the E.U.; and (2) when employing individuals based in the E.U.

An employer with HR functions based in the E.U. will be subject to GDPR because the employer – through its HR functions – is collecting data within the E.U. This seems simple enough. The key takeaway here is that GDPR arguably applies to *all* data collected by the E.U.-based functions, including data collected on U.S.-based individuals. Put into context, if a

U.S. company's HR functions are based in the E.U., then GDPR applies to the data collected in connection with *all* applicants and employees, including the applicants and employees based in the U.S. This is because the HR functions are based in the E.U. and therefore, at a minimum, involve the collection and processing of data within the E.U.

Employing individuals based in the E.U. will also trigger GDPR. This is because the employer reaches into the E.U. to collect data on these E.U.-based employees or independent contractors (ICs). This, again, seems simple enough. The key takeaway is that GDPR continues to apply even when E.U.-based employees or ICs telecommute in connection with entirely U.S. operations. Because data is collected on the employees or ICs while they are physically in the E.U., GDPR applies.

Does GDPR cover employees from the E.U.?

Not likely. GDPR does not apply based on the nationality or citizenship of an individual. GDPR's application is location based – i.e., where a company operates, has a presence, or otherwise collects, processes, and stores data. For this reason, collecting data on an employee or IC living and working in the U.S. does not, by itself, trigger GDPR. This is true even if the U.S.-based employee or IC is an E.U. citizen or has dual citizenship, and even if the employee or IC is in the U.S. on a work permit or visa. Taken together, if a company is not otherwise subject to GDPR – again, check out our webinar series on general coverage issues – then collecting data on an employee or IC living and working in the U.S. will not trigger GDPR. This changes, however, if the employee or IC splits his or her time between the U.S. and the E.U. That situation is extremely fact specific, and we would need additional information before we could provide further advice.

We don't collect data on our employees – so GDPR doesn't apply?

All employers collect "data" on their employees, at least in the context of GDPR. GDPR defines data several different ways, and its definitions do not always fit neatly with how we in the U.S. think of private information, especially in the employment context. Under GDPR, "personal data" includes virtually everything related to an individual from his or her name, to online information, to "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of the individual. GDPR then goes on to define "sensitive personal data," which includes "religious or philosophical beliefs," "genetic data," and "data concerning health or sex life and sexual orientation." Obviously, given its nature, employers avoid even learning about "sensitive personal data," much less collecting it. That said, employers routinely collect, process, and store "personal data" on all of their employees. As a result, it would be nearly impossible to argue that employers do not collect "data" under GDPR.

Which federal agency will enforce GDPR in the employment context? The DOL? The EEOC? Which one?

None of the federal agencies that employers deal with on a day-to-day basis have any enforcement or regulatory authority with respect to GDPR. This is good news. But GDPR cannot be viewed strictly from the standpoint of HR or employment practices. GDPR is absolutely a "whole company" issue and one that needs to be looked at closely.

GDPR applies to my company. Now what?

There is no one-size-fits-all answer, and even then, answers will vary based on the nature and sophistication of the company. Broadly stated, your company needs to be made GDPR compliant. We typically start this

process with an audit that identifies any gaps in compliance and suggestions for how to fill those gaps moving forward. From there, we revise relevant policies and update necessary forms. For example, GDPR requires privacy notices. In the employment context, these notices are similar to the disclosures employers must provide employees under the Fair Credit Reporting Act. Once the policies and necessary forms are updated, they are implemented in connection with training and information sessions, just like with any other new policy or practice. Again, the changes a company needs to make will depend on the nature and sophistication of the company.

Even if GDPR does not apply to your company, it still provides useful guidance and best practices on the collection and storage of all types of data. For more information on the topics in this article or GDPR in general, please contact the author, Zachary Busey, or any member of Baker Donelson's GDPR team.