MORSE
BARNES-BROWN
PENDLETON

Client Alert:

4 *SCARY* Facts about the New European Union General Data Protection Regulation

By Faith D. Kasparian

This Halloween, in the privacy and data security world, it is not the ghost or goblin that should frighten your business – but rather, the looming May 25, 2018 deadline for compliance with the new European Union General Data Protection Regulation (GDPR). In honor of Halloween, MBBP's privacy and data security team shares the following list of 4 SCARY facts about the GDPR.

1. ***The GDPR Reaches Businesses Outside the EU.*** The expansive scope of the GDPR applies not only to businesses in the EU, but also to the processing of personal data of EU residents *by businesses outside the EU*, where the processing relates to: (a) offering goods or services to individuals in the EU, or (b) monitoring behavior of individuals in the EU. (*Note*: "Processing" includes *any type* of collection, disclosure, handling, storage, or other use of personal data; "personal data" means any information relating to an identified or identifiable natural person – and would include even a business e-mail address as well as information that many in the United States may not consider personally identifiable.

2. ***The GDPR Imposes Liability Directly on Businesses That Process Personal Data For Another Business.*** Unlike the existing EU regulatory scheme, under the GDPR, businesses that simply "process" (broadly defined as above) personal data on behalf of another business are *directly liable for GDPR compliance*.

3. ***The GDPR May Impose Substantial Fines For Non-Compliance.*** For certain violations of the GDPR, the fine may be the higher of (a) EUR 10,000,000, or (b) 2% of the violator's total worldwide annual turnover. *For other violations (including inappropriate transfer of personal data to a country that lacks "adequate" data protection, such as the United States), the fine may be the higher of (c) EUR 20,000,000, or (d) 4% of total worldwide annual turnover*.

4. ***If You Are In The B2B Space, Your EU Customers Cannot Do Business With You.*** Under the GDPR, a business may only allow another business to "process" personal data if the processor complies with the GDPR and contractually agrees to certain stipulations. *Ultimately, those in the business-to-business space (including SaaS and other business service providers) that handle information about their customers' EU customers or EU employees (even simply business contact information) will need to comply with GDPR if they want to continue doing business beyond May 24, 2018*.

Rather than being paralyzed with fear, companies should take proactive steps to comply with the GDPR, including by ensuring that they have appropriate EU-U.S. data transfer mechanisms in place. If you have questions about these matters, ***"Who you gonna' call?"*** Our privacy and data security team – Faith Kasparian (CIPP-U.S.) at *fkasparian@mbbp.com*, Amanda Schreyer at *aschreyer@mbbp.com*, Mike Cavaretta at *mcavaretta@mbbp.com*, Jamie Dalton at *jdalton@mbbp.com*, and Howard Zaharoff at *hzaharoff@mbbp.com* – of course!