
# The Impact of GDPR on Attorneys and Law Firms in the United States

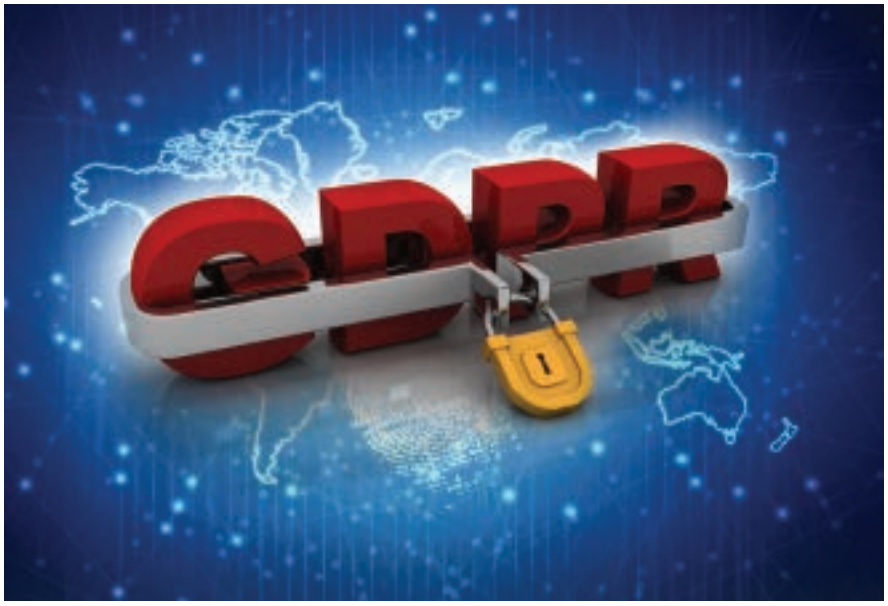
By Sean McGuinness and Katie Fillmore

It is fair to say that by now U.S. attorneys should be somewhat familiar with the new General Data Protection Regulation ("GDPR") requirements. We all have received numerous e-mails from various parties advising of new data privacy regimens. In addition, just casually surfing the Internet will bring pop-up notifications of data privacy updates. These are all related to what is called GDPR.

## What is GDPR and how does it impact American businesses?

On May 25, 2018, the European Union's GDPR took effect. Although European Union ("EU") laws typically don't have a worldwide impact, the GDPR will impact businesses across the globe, including law firms/attorneys based in the United States. The GDPR has an extremely broad application, as it was adopted as an effort to hold businesses, including those outside of the EU, accountable for the use and protection of data belonging to EU citizens. As gaming is a worldwide industry, most U.S. gaming attorneys and law firms have clients (or individuals that are associated with a client entity) that have protected EU status under the GDPR. It also would apply to casinos in the U.S. that have EU citizen customers/patrons.

*Continued on next page*




*Continued from previous page*

## Applicability

The GDPR applies not only to European entities, but also applies to entities located outside of the EU that offer goods or services to people in the EU or that monitor the behavior of people in the EU. Clearly, this would also apply to U.S. based law firms/attorneys as any business with EU resident customers/clients is required to comply. The GDPR applies to businesses offering goods or services to EU residents, regardless of whether payment for the good or service is required. As such, even a *pro bono* representation is implicated if it collects data from or monitors EU residents. The GDPR applies to both controllers (defined as an entity that determines why and how personal data is being collected) and processers (defined as an entity that processes the data on behalf of the controller). A law firm would fall into these categories, especially if it does gaming licensing work for EU citizens. Of course, a U.S. casino with EU citizen customers/patrons would also be subject to the GDPR.

## Covered Data

The GDPR regulates "personal data" which is defined as any information related to a natural person or data subject that can be used directly or indirectly to identify that person. Personal data includes, for instance, a name, photo, email address, bank details, medical information, GPS location data, and IP address. Clearly, gaming applicants that are EU citizens would need to share personal data to gaming regulators. Accordingly, U.S. based attorneys/firms with such clients need to comply with the GDPR. This is also the case with U.S. casinos with EU citizen customers/patrons.

## Enhanced Privacy Rights

The GDPR significantly increases data privacy obligations, increases penalties, including fines as high as the greater of 20 million euros or four percent of annual worldwide revenue. One should anticipate that the GDPR is likely to increase enforcement activity, although it is not yet clear exactly how this will be done. The significant enhancements referenced above include the following:

**Consent:** Controllers and processors are required to be transparent with how information is used and, as a general rule, consent must be obtained from the individual. The request for consent must be in clear, plain language. Simply asking an individual to accept a privacy policy that is not provided is not sufficient.

**Rectification/Erasure of Data:** The GDPR confers rights to an individual to access his or her own data and rectify/erase inaccurate data.

**Assessments:** Controllers are mandated to conduct data protection impact assessments, involving routine evaluation of the potential impact of lost or diverted data.

**Breach Notification:** The GDPR mandates breach notification within 72 hours of awareness of the breach if the breach is likely to result in a risk for the rights and freedoms of individuals.

Indeed, we are starting to see gaming companies with EU citizens that would need to be licensed in the U.S. sending data privacy questionnaires to U.S. law firms/attorneys (in addition to requesting W-9 and typical vendor compliance diligence information). These address identifying what sort of personal information the law firm/attorney may be receiving; what jurisdictions that law firm/attorney will be using the personal data and what protocols would be in place for the EU citizen to receive notification concerning the date and where it is being transmitted to, as well as what security measures are in place to protect the personal data.

As mentioned above, the economic sanctions for noncompliance have the potential of being steep. The amount of the fine will vary depending on what provision is breached and the behavior of the organization, with the purpose of imposing an amount which is effective, proportionate, and dissuasive. EU residents can enforce the GDPR's protections by lodging a complaint with the supervisory authority of the EU member state or by filing an action if the supervisory authority fails to address the complaint properly. Additionally, an EU resident may take direct action through class action proceedings. Thus, increased litigation of privacy issues in the EU is likely.

## Legal Ethics Considerations

An aspect that hasn't been discussed much concerning the GDPR's applicability to U.S. law firms/attorneys is the applicability of legal ethics requirements administered by the various state bars in the U.S. Canon 4 states that a lawyer should preserve the confidences and secrets of a client. Certainly, the personal data of an EU citizen/client would fall under this canon. Similarly, Rules 1.6 (Confidentiality of Information) and 1.15 (Safekeeping Property) of the ABA Model Rules of Professional Responsibility would add the possibility of legal discipline from a state bar authority for non-compliance with the GDPR. Certainly an adverse GDPR action against a U.S. law firm/attorney would be problematic in a state bar disciplinary action concerning non-compliance with the GDPR (and any law firm/attorney should expect that if a legal action is made pursuant to the GDPR that a corresponding bar complaint would follow).

> **"The GDPR is arguably the most significant data privacy regulation that has been enacted to date, and the full breadth of GDPR is far beyond the scope of any article."**

## Compliance Tips

Given the expansive application of the GDPR and the practical difficulty of differentiating citizenship (there can be situations with individuals with dual citizenship) among customers/clients, many companies/law firms with worldwide operations/clients have opted to apply the GDPR principals to the management of all customer/client data. By comparison, the U.S. does not currently have an omnibus federal law regulating the collection, use, and disclosure of personally identifiable information ("PII"), but there are several sector-specific laws, such as the Health Insurance Portability and Accountability Act ("HIPAA") applying to the use and disclosure of personal health information. However, all 50 states in the U.S. have enacted data protection laws, primarily governing cyber breaches. For a business with global operations, there is a patchwork of potentially applicable law and regulation. Defining a privacy policy that meets the most stringent requirements may likely be the best approach.

As an initial step, it is critical that companies/law firms conduct a comprehensive review of data collection and processing to ensure compliance with all applicable laws. Companies should consider what information is collected, why, and whether collection is necessary. Also, they should evaluate what privacy laws are implicated, both domestically at the state and federal level and abroad. The international gaming company's data privacy questionnaire referenced above is helpful in this regard. Companies should also stay up to date with changes in the law, including interpretations in case law, agency guidance, and enforcement actions.

Additionally, companies/law firms should revise privacy statements and requests for consent. All customer-facing documentation will require revision to comply with the GDPR, which requires providing detailed information to data subjects regarding the processing of personal data in a concise, transparent, intelligible, and easily accessible form.

Companies may also want to invest in an insurance policy that provides cyber coverage, including protection for data breaches. Many traditional general liability insurers have added cyber liability exclusions to their policies. Companies should carefully read the terms of their insurance policies to fully understand what is covered and consider purchasing additional insurance.

## Conclusion

The GDPR is arguably the most significant data privacy regulation that has been enacted to date, and the full breadth of GDPR is far beyond the scope of any article. It is essential that law firms/attorneys take the time to understand the various requirements and take steps to ensure compliance with the GDRP as well as other applicable data privacy laws. In this regard, it would be helpful to reach out to European lawyer colleagues whose firms may have experience in dealing with the GDPR. ♣

Sean McGuinness

Katie Fillmore

*Sean McGuinness is a partner at Butler Snow LLP. He practices gaming law on a multi-jurisdictional basis and is licensed to practice in Nevada, Colorado, Iowa and Mississippi. He can be contacted at sean.mcguinness@butlersnow.com*

*Katie Fillmore is an attorney with the Austin, Texas, office of Butler Snow LLP. Her practice is focused on defense of tort and product liability cases, as well as general commercial litigation. She can be reached at Katie.Fillmore@butlersnow.com.*