PUBLICATION

A GDPR Check-up for U.S.-Based Hospitality Businesses

May 24, 2018

The U.S. hospitality industry is eager to know how European Union Regulation 2016/679, more commonly known as the General Data Protection Regulation (GDPR), will impact it, especially with respect to the guest experience, internal operations, marketing efforts, and vendor relationships. With the GDPR enforcement deadline fast approaching on May 25, 2018, every business that offers goods or services to or collects behavioral data from European residents should have already determined whether the GDPR is likely to apply to its operations and considered whether and how it intends to address the GDPR's compliance obligations. For most businesses, the prospect of erasing legacy personal data to avoid GDPR compliance is simply infeasible (although U.K.-based pub chain J.D. Wetherspoon reportedly exercised this option by deleting their entire customer email database) and ignoring GDPR compliance obligations may not only prove illegal, but invite hefty financial penalties amounting up to the greater of €20 million or four percent of the businesses' worldwide annual revenue for the prior fiscal year.

For those U.S.-based hospitality businesses working towards GDPR compliance, here is a summary of key concepts and considerations to keep in mind as the deadline for enforcement approaches.

Guests are your primary, but not only, data subjects and sources of personal data. Your guests are likely to provide you with many types of personal data as they navigate your businesses' reservation, check-in, sales, billing, and customer relationship processes; in doing so, they are your primary sources of personal data, especially in terms of data complexity and volume. This personal data reaches your business through a variety of methods (fax, email, telephone, websites, paper forms, etc.) and data collection points (reservation and distribution systems, loyalty programs, and social media accounts), to name a few. On any given day, you are highly likely to be collecting other personal data from your businesses' employees, vendors, service providers, suppliers, independent contractors, and business partners.

What you may not realize is that all of these individuals and entities are capable of providing you with personal data subject to the GDPR. The regulation is currently written in such a way that it is expected to be interpreted to include not only the personal data of individuals but also business-to-business data that identifies an individual (e.g., a business email address like annsmith@company.uk, but not sales@company.uk).

How does personal data differ from PII? As a U.S.-based business that handles a wide variety of guest data, you are probably already familiar with the concept of "personally identifiable information", or "PII", as this term is widely used throughout the bundle of laws that comprise the U.S. privacy law landscape. The term "PII" does not have a uniform meaning across U.S. privacy law, but generally includes such personal identifiers such as name, date of birth, telephone or mobile phone numbers, email addresses, social security numbers, and bank account numbers, at a minimum. In fact, some U.S. privacy laws include less obvious personal identifiers within the definition of PII, such as Internet Protocol (IP) and MAC device addresses (which identify an individual's computer) and biometric records.

Under the GDPR, the concept of "personal data" is even broader than the concept of PII under U.S. privacy law. It includes any information relating to "an identified or identifiable natural person" (also known as a "data subject"). Chances are that you already identify your guests by assigning them an "identifier" whenever they

book a hotel room, a conference room, a restaurant reservation, or a spa service through your business or business partners. It is also likely that you already track and solicit data from your employees, independent contractors, and business partners for human resources, vendor management, and other purposes.

The broad range of "identifiers" relevant to GDPR compliance include: "name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Now think about all of the non-obvious ways in which guests, employees, independent contractors, business partners, and others may be sharing such information with your business. For example, whenever an individual registers for or attends a trade event at or through your business, they are likely to reveal certain identifying factors about themselves, which may include health, sexual orientation, racial or ethnic identity, political beliefs, or religious views. In fact, during such events, your business also may be collecting personal data about these individuals through photography, video footage (including surveillance by closed-circuit television), social media, and customer lifestyle profiling. By collecting and storing this data, your business can create GDPR obligations for itself.

Some good news: Preparing for GDPR might require less work than you think. Most hospitality businesses operating in the United States already have certain privacy and security measures in place to prevent the unauthorized disclosure or loss of PII. Fortunately, that PII is likely to be a subset of the personal data required to be protected under the GDPR. In fact, some privacy and security concepts common to GDPR and U.S. privacy law compliance include "privacy by design" (a longstanding principle applicable to the design and architecture of IT systems and associated business practices), end-to-end encryption of personal data, access controls, data retention and destruction, and privacy disclosures, online and offline. Also, hospitality businesses that already comply with the Payment Card Industry Data Security Standard (PCI DSS) will have a head start on preparing for the GDPR as compared with businesses that are not PCI compliant. Therefore, businesses that already have comprehensive data privacy and security measures and policies in place will be well-poised to implement GDPR compliance.

Clear, specific, and unambiguous consent is king. Whenever a data subject consents to the processing of his or her personal data, incorporate language that solicits and documents that consent and accurately states each and every purpose for the data processing. Be aware that your business will need to solicit consent whenever the purpose and scope of a data subject's consent changes. Also, when a data subject consents to booking a service through a third party, such as a travel agent, that consent may be distinguishable from the consent required for your business to conduct further data collection and processing activities. It is always best to obtain consent from the data subject directly and independently.

Beyond consent, the GDPR also provides that personal data processing may be conducted if another lawful basis for such processing exists, such as a contractual obligation, a legal obligation, a vital interest necessary to protection of an individual, an exercise of official (public or government) authority, a legitimate interest (which is subject to a balancing test between the purpose of the data processing and the data subject's interests, rights, and freedoms). A business seeking to rely on any of the foregoing bases for personal data processing must clearly document each and every basis for such processing, which can pose a considerable operational burden. Also, be mindful that certain "special" categories of sensitive data (such as race, ethnic origin, trade union membership, and biometrics) and criminal offense records are subject to further processing restrictions and approvals from E.U. officials.

Broader guest rights. A more comprehensive menu of rights will be available to your guests (and other data subjects) under the GDPR, including: (i) the right to access, rectify, and erase one's personal data, (ii) the right to erase one's data (also known as "the right to be forgotten"), (iii) the right to restrict or object to data processing, (iv) the right to transfer one's data to another party (also known as "data portability"), and (v) the right to prohibit or revoke consent to marketing initiatives or profiling.

Compliance with data subject requests will need to be timely addressed (within 72 hours or less) and processing will need to be conducted in a manner that is adequate, relevant, necessary, and appropriate to the purpose(s) to which the data subject consented or are otherwise allowed under the GDPR.

Updating your contracts. As part of its GDPR compliance, your business will need to inventory and update its contracts, policies, and disclosures relevant to the processing of personal data. This will include, but not be limited to: privacy policies and disclosures (both online and offline), customer and vendor contracts, operating manuals, franchise agreements and franchise disclosure documents, internal policies and procedures (especially those concerning vendor management and safeguarding of personal data), compliance checklists, and employee and subcontractor training materials.

A major change under the GDPR relates to its requirements for third party data processing agreements. Such agreements must address the data processing roles (controller, processor, or joint controller) to be assumed by your business as well as any third parties to the agreement and specify the obligations and liabilities associated with each role. Also, in the interest of transparency, any customer-facing notices, contracts, and websites in use by your business will need to be concise and easy-to-understand under GDPR. Given this, your business should seek legal or other expert advice when updating its documentation for GDPR compliance, especially since you can reasonably expect some third parties to question whether GDPR applies to your U.S.-based business.

As your U.S.-based hospitality business prepares for the advent of the GDPR, it will need to consider the above concepts and considerations as part of its larger GDPR compliance strategy. It is also important to recognize that E.U. member states may enact local laws that limit or extend the purview of the GDPR and the GDPR is not the only foreign data protection regulation that may impact your business. Other potentially relevant data protection regulations have been and will continue to be enacted by foreign nations, at regional and local levels.

If you have questions about GDPR compliance, contact any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.