THE
NATIONAL LAW REVIEW

Don’t Gamble with the GDPR

Friday, April 20, 2018

The European Union’s (EU) General Data Protection Regulation (GDPR) goes into effect on May 25, and so do the significant fines against businesses that are not in compliance. Failure to comply carries penalties of up to 4 percent of global annual revenue per violation or $20 million Euros – whichever is highest.

This regulatory rollout is notable for U.S.-based hospitality businesses because the GDPR is not just limited to the EU. Rather, the GDPR applies to any organization, no matter where it has operations, if it offers goods or services to, or monitors the behavior of, EU individuals. It also applies to organizations that process or hold the personal data of EU individuals regardless of the company’s location. In other words, if a hotel markets its goods or services to EU individuals, beyond merely having a website, the GDPR applies.

The personal data at issue includes an individual’s name, address, date of birth, identification number, billing information, and any information that can be used alone or with other data to identify a person.

Article By Dickinson Wright PLLC
Sara H. Jodka
International (Newsletters & Client Alerts)

Communications, Media & Internet
Global
Entertainment, Art & Sports
All Federal
European Union

The risks are particularly high for the U.S. hospitality industry, including casino-resorts, because their businesses trigger GDPR-compliance obligations on numerous fronts. Hotels collect personal data from their guests to reserve rooms, coordinate event tickets, and offer loyalty/reward programs and other targeted incentives. Hotels with onsite casinos also collect and use financial information to set up gaming accounts, to track player win/loss activity, and to comply with federal anti-money laundering “know your customer” regulations.

Privacy Law Lags in the U.S.

Before getting into the details of GDPR, it is important to understand that the concept of privacy in the United States is vastly different from the concept of privacy in the rest of the world. For example, while the United States does not even have a federal law standardizing data breach notification across the country, the EU has had a significant privacy directive, the Data Protection Directive, since 1995. The GDPR is replacing the Directive in an attempt to standardize and improve data protection across the EU member states.

Where’s the Data?

Probably the most difficult part of the GDPR is understanding what data a company has, where it got it, how it is getting it, where it is stored, and with whom it is sharing that data. Depending on the size and geographical sprawl of the company, the data identification and audit process can be quite mind-boggling.

A proper data mapping process will take a micro-approach in determining what information the company has, where the information is located, who has access to the information, how the information is used, and how the information is transferred to any third parties. Once a company fully understands what information it has, why it has it, and what it is doing with it, it can start preparing for the GDPR.

What Does the Compliance Requirement Look Like in Application?

One of the key issues for GDPR-compliance is data subject consent. The concept is easy enough to understand: if a company takes a person's personal information, it has to fully inform the individual why it is taking the information; what it may do with that information; and, unless a legitimate basis exists, obtain express consent from the individual to collect and use that information.

In terms of what a company has to do to get express consent under the GDPR, it means that a company will have to review and revise (and possibly implement) its internal policies, privacy notices, and vendor contracts to do the following:

- Inform individuals what data you are collecting and why;
- Inform individuals how you may use their data;
- Inform individuals how you may share their data and, in turn, what the entities you shared the data with may do with it; and
- Provide the individual a clear and concise mechanism to provide express consent for allowing the collection, each use, and transfer of information.

At a functional level, this process entails modifying some internal processes regarding data collection that will allow for express consent. In other words, rather than language such as, "by continuing to stay at this hotel, you consent to the terms of our Privacy Policy," or "by continuing to use this website, you consent to the terms of our Privacy Policy," individuals must be given an opportunity not to consent to the collection of their information, e.g., a click-box consent versus an automatically checked box.

The more difficult part regarding consent is that there is no grandfather clause for personal information collected pre-GDPR. This means that companies with personal data subject to the GDPR will no longer be allowed to have or use that information unless the personal information was obtained in line with the consent requirements of the GDPR or the company obtains proper consent for use of the data prior to the GDPR's effective date of May 25, 2018.

What Are the Other "Lawful Basis" to Collect Data Other Than Consent?

Although consent will provide hotels the largest green light to collect, process, and use personal data, there are other lawful basis that may exist that will allow a hotel the right to collect data. This may include when it is necessary to perform a contract, to comply with legal obligations (such as AML compliance), or when necessary to serve the hotel's legitimate interests without overriding the interests of the individual. This means that during the internal audit process of a hotel's personal information collection methods (e.g., online forms, guest check-in forms, loyalty/rewards programs registration form, etc.), each guest question asked should be reviewed to ensure the information requested is either not personal information or that there is a lawful reason for asking for the information. For example, a guest's arrival and departure date is relevant data for purposes of scheduling; however, a guest's birthday, other than ensuring the person is of the legal age to consent, is more difficult to justify.

What Other Data Subject Rights Must Be Communicated?

Another significant requirement is the GDPR's requirement that guests be informed of various other rights they have and how they can exercise them including:

- The right of access to their personal information;
- The right to rectify their personal information;
- The right to erase their personal information (the right to be forgotten);
- The right to restrict processing of their personal information;
- The right to object;
- The right of portability, i.e., to have their data transferred to another entity; and
- The right not to be included in automated marketing initiatives or profiling.

Not only should these data subject rights be spelled out clearly in all guest-facing privacy notices and consent forms, but those notices/forms should include instructions and contact information informing the individuals how to exercise their rights.

What Is Required with Vendor Contracts?

Third parties are given access to certain data for various reasons, including to process credit card payments, implement loyalty/rewards programs, etc. For a hotel to allow a third party to access personal data, it must enter into a GDPR-compliance Data Processing Agreement (DPA) or revise an existing one so that it is GDPR compliant. This is because downstream processors of information protected by the GDPR must also comply with the GDPR. These processor requirements combined with the controller requirements, i.e., those of the hotel that control the data, require that a controller and processor entered into a written agreement that expressly provides:

- The subject matter and duration of processing;
- The nature and purpose of the processing;
- The type of personal data and categories of data subject;
- The obligations and rights of the controller;
- The processor will only act on the written instructions of the controller;
- The processor will ensure that people processing the data are subject to duty of confidence;
- That the processor will take appropriate measures to ensure the security of processing;
- The processor will only engage sub-processors with the prior consent of the controller under a written contract;
- The processor will assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- The processor will assist the controller in meetings its GDPR obligations in relation to the security of processing, the notification of personal data breaches, and data protection impact assessments;
- The processor will delete or return all personal data to the controller as required at the end of the contract; and that
- The processor will submit to audits and inspections to provide the controller with whatever information it needs to ensure that they are both meeting the Article 28 obligations and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Other GDPR Concerns and Key Features

Consent and data portability are not the only thing that hotels and gambling companies need to think about once GDPR becomes a reality. They also need to think about the following issues:

- *Demonstrating compliance.* All companies will need to be able to prove they are complying with the GDPR. This means keeping records of issue such as consent.
- *Data protection officer.* Most companies that deal with large-scale data processing will need to appoint a data protection officer.
- *Breach reporting*. Breaches of data must be reported to authorities within 72 hours and to affected individuals “without undue delay.” This means that hotels will need to have policies and procedures in place to comply with this requirement and, where applicable, ensure that any processors are contractually required to cooperate with the breach-notification process.

Source URL: https://www.natlawreview.com/article/don-t-gamble-gdpr