PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Is GDPR Inhospitable to Hospitality?

What Industry Leaders Need to Know to Protect Their Organizations, Market Share, Clients and Profits

By Clare E. Cella, Partner, Hospitality Practice and Thomas J. DeMayo, Principal, Cyber Risk Management

The EU's new General Data Protection Regulation, known as GDPR, requires businesses to capture and manage customer data in entirely new and complex ways. It requires that they interact with clients according to very specific and time-consuming requirements and are sensitive to their privacy rights and freedoms. Regardless of where they are headquartered, organizations with EU-based customers or prospects may have to comply. In addition, they may have to appoint a representative within the organization to assume full responsibility for fulfilling GDPR's many requirements.

Certainly, these are laborious tasks that require significant time, knowledge and attention to detail. The opportunities, however, are well worth the investment of time and money. In an age when privacy is a high-priority hot button issue, organizations are wise to commit to protecting their constituents' confidentiality. In fact, it is difficult to quantify the advantages this offers to those who champion the virtues of consumer privacy and establish a framework of corporate responsibility, consumer safety, education and awareness.

GDPR Affects the Entire Hospitality Industry

All companies and organizations that operate in the EU or that provide or plan to offer goods or services to constituencies in the European Union are required to comply fully with GDPR, which went into effect on May 25, 2018. The regulation applies to all travel agencies, tour operators, hotels, motels, inns, clubs, bed-and-breakfasts, Airbnbs, automobile rental agencies, restaurants, aggregators and other travel and hospitality groups that operate in Europe – or to groups that operate outside of the EU and actively maintain information on and market their services to EU residents. The requirement is an opt-in one for EU consumers, which often requires them to actively agree and to be provided complete transparency regarding how their personal information is kept and used. As the requirements are based on where consumers *currently* reside, protection applies to the personal information of American expatriates and exchange students living in the EU as well as to EU residents booking U.S. travel.

Critical Questions

- What personally identifiable information do you collect or store?
- Do you collect political, religious, health or other sensitive data?
- Do you collect data on children?
- Have you secured consent to collect this data?
- Do you tell customers why you are collecting this data and how you will use it?
- Can you prove that your EU-based customers have opted in to data collection?
- Have you informed customers that they may withdraw consent at any time? Do you have a process for doing so?
- Have you removed non-responders from your database?

Noncompliance can result in hefty fines, operational setbacks and reputational damage. As a result, it's imperative that all industry entities are fully invested in addressing the policies, procedures and technology employed to handle personally identifiable information (PII) by their management, staff and third parties.

Personalization: The Benefits and Risks

GDPR is designed to prevent the misuse of an individual's personal information and to protect the individual's rights by limiting how that information is used. As a result, it covers any information that allows an EU resident to be personally identified whether included in a membership, client or prospect database – a prodigious amount of information in an industry characterized by the demand for a high degree of personalization.

Hotel guests often anticipate that their particular needs and expectations will be attended to, which requires that this information is maintained and updated in internal or external databases. Travelers expect to receive rewards based on their current status in affinity programs, necessitating regular updates to additional up-to-the-minute databases.

Online travel agents like Expedia, Booking.com, Travelocity, Kayak and others appeal to customers by offering attractive discounts they secure by reserving rooms in block quantities. These booking aggregators typically provide hotels with minimal information such as name, room type and dates of stay – but not e-mail addresses, which they avoid sharing in order to enlarge their own private marketing databases. However, the fact that limited information is shared does not exclude the hotel from protecting the guest information it acquires. Further, because the hotels receive limited information from the online travel agents, they often implement tactics to obtain additional information, such as the e-mail address, and to entice the guest to book directly with the hotel for future stays. These tactics to sway customer booking decisions should be evaluated to ensure they are transparent and not invasive. Hotels, aggregators and agents must all comply with GDPR requirements, particularly when data will be used for marketing purposes.

Third-Party Vulnerability

Additional exposure accompanies the use of third-party partners. Although critical to providing supplementary amenities, marketing support, website development and maintenance, legal and operational resources, external vendors can also prove to be a business's weak spot when it comes to data protection. Under GDPR, for example, a hotel will be held accountable should a breach occur at a firm to which it has outsourced data processing. The reason is that the regulation identifies organizations by category – data controllers or data processors. An entity can be one or the other – but it can also be both, thus upping the ante for noncompliance.

Simply stated, *controllers control*; they determine why and how consumers' personally identifiable information is used. Although they don't necessarily store or process data, they are still fully responsible for how data is maintained, employed and deleted even when handled by a third party. An inn that collects the preferences and contact information for loyal clients is considered a controller whether it stores the data on its own or through an outside firm.

Similarly, *processors process*; they store data, often but not always on a third-party server – and then manage, sell or otherwise manipulate that data for the controller or for themselves. Examples include: external payroll processors; market research firms; affinity programs that sell to member bases such as hotel rewards programs; aggregators that market their own and others' products and services to the consumer.

This layered complexity adds layers of responsibilities that must be met. Management must be educated about GDPR's requirements and implications. Staff must be trained to handle data – and customers – properly. Websites, privacy policies and communications materials must be reviewed and revised. Third-party resources must be vetted, software customized, contracts, procedures and processes analyzed and updated. Breaches must be reported to both authorities and those affected within 72 hours. Combined, these tasks, and others, create an onerous burden, which is why many organizations rely on experienced specialists for guidance and support.

Critical Questions

- Where is data physically stored?
- How is access to data controlled?
- How do you protect this data?
- Can you encrypt and/or pseudonymize it?
- Do you review the data regularly to ensure it is not being held longer than necessary?
- What software do you use?
- How does that software interact with outside vendors?
- Do vendors adequately protect this data?

How to Comply

Despite the fact that GDPR is a regulation, not a law, hospitality organizations are wise to treat it as though it were mandatory given the potential for reputational damage and sizable financial penalty.

A key step is to undertake a **Data Protection Impact Assessment** (DPIA) to identify and address risks before they become problematic. The analysis examines existing internal controls, contractual agreements with service providers, security threats and business factors. This is especially valuable in cases where the introduction of new data processing technologies may pose increased risk to consumers.

Equally valuable is the creation of a detailed blueprint, a **Data Governance Framework**, that integrates security throughout the organization and specifies roles, responsibilities, policies and processes. It details procedures for data warehousing and classification, pseudonymization, responding to consumer requests, staff training, external security testing, solutions application, risk mitigation and a step-by-step action plan in the event of a threat, breach, intrusion or hack.

These essential steps, and others, are made less challenging with the help of experts who have specialized in understanding and complying with GDPR since before the regulation took effect. Such professionals can also assist with implementing a re-consent e-mail program, re-architecting CRM systems for more accurate and compliant data capture and establishing a Geofence to enhance customer data protection by managing EU-based cookies and consent requirements.

Critical Questions

- Who within your organization needs to understand GDPR?
- Have you trained staff to handle data safely?
- Who is responsible for implementing and maintaining appropriate data management processes and policies?
- Is your privacy policy current, complete, properly disseminated?
- Are you prepared to honor requests for data portability, correction or deletion?
- What external testing takes place to confirm data security?
- How would you report a data breach?
- To whom can you turn with questions?

The Case for Expert Support

Like other businesses, hospitality firms must weigh the risks against the costs associated with both compliance and noncompliance. GDPR-imposed fines and fees can reach €20,000,000 /$23,944,000 or 4% of the organization's worldwide revenues for the preceding year, whichever is higher. While the financial and reputational risks are indisputably punishing, collaborating with experienced specialists can help ensure that the overall expense is surprisingly affordable and, most important, adds significant value. Advisors at qualified professional services firms are well-versed in the nuances of GDPR as well as IT risk advisory, cybersecurity, digital forensics and technology systems design. The ideal partner also delivers access to specialists, regulators and government officials around the world, particularly in the European Union and United Kingdom.

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today's* 2018 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today*. In 2018, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.

Contact Us

Clare E. Cella, CPA
Partner, Hospitality Practice
212.867.8000 | ccella@pkfod.com

Thomas J. DeMayo, CISSP, CISA, CIPP/US, MCSE, CEH, CHFI
Principal, Cyber Risk Management
212.286.2600 | tdemayo@pkfod.com