HOTEL ONLINE

Guests from the European Union Could Soon Cost Unprepared Hoteliers

February 2, 2018 10:26am

By John Barchie

As of May 25, 2018, hotels accepting reservations from citizens of an European Union (EU) country could be at risk for fines, depending on how those reservations were made. This is because hotels may fall under the purview of the new General Data Protection Regulation (GDPR) when it takes effect.

GDPR was designed to better protect EU citizen data and ensure that companies storing that data should possess it. Standards vary based on where the data originates from, but generally any information like name, address, credit card number, etc. is covered. In the domestic U.S., protected data is defined as Personally Identifying Information (PII). And, as defined by GDPR, for an EU citizen it is known as Personal Data. Failure to protect the PII or Personal Data to the right standard could bring a hefty bill, or upon consistent failure, even an order to cease business in EU countries.

Current U.S. based data privacy regulations require companies to notify customers if a data breach occurs, but in the U.S., there can be a significant time delay between the breach and the notification letter, not so with GDPR. GDPR requires the Supervisory Authorities be notified within 72 hours, even while a breach is still being investigated. Failure to report within 72 hours could lead to significant fines. Maximum fines could be up to $26MM or 4% of global gross revenue, whichever is greater.

Hotels may be affected by the complexity of GDPR because, similar to travel companies, they gather credit card PII and Personal Data from EU subjects. So, essentially, if an EU citizen plans to come to the U.S. on vacation and engages in the transaction from the EU or via an EU website then the hotel may be subject to GDPR if the transaction consent form is not properly worded. That's right, GDPR requires a consent form prior to processing EU citizen's personal data.

The first step toward compliance for hotels is determining the need for and if necessary, assigning a Data Protection Officer (DPO). A company will be required to have a DPO if it processes large sums of data covered by GDPR. This person must be available and involved in any events where there is a possibility of a loss of GDPR covered data. The DPO will be the point person for any GDPR issue with the affected persons and the Supervisory Authority. Obviously, because the DPO will be instrumental in proving your company's compliance with GDPR this individual needs to know the regulations and your security protocols inside and out, backward and forward. If your company is not required to have a DPO, you should still have a plan in place for who you will call if the Supervisory Authority opens an investigation.

Of course, hotels cannot stop there. All Personal Data needs to be evaluated to determine if the business is legally allowed to receive, store, or process the data. Any unlawful possession of data covered under GDPR will be viewed as a serious violation. Any Personal Data that is lawfully received, stored or processed by a company needs to be encrypted. This means completely encrypted at rest and in transit, complete end to end encryption. All of these efforts need to be documented so they can be given to a Supervisory Authority upon request.

There are many other components of GDPR that companies should familiarize themselves with and comply to if required. The best source of information on the regulation requirements is gdpr-info.eu.

Once GDPR takes effect, if a hotel experiences a breach or is contacted by a GDPR Supervsiory Authority the best course of action is to show an attitude of compliance by offering complete support for the investigation. Then, contact the legal team. It is important to remember that complying with GDPR can be complex. It takes some time to update systems and processes to the level of security required by the new regulations. It can also be costly, and distruptive, but the protection of data is becoming paramount in the new business paradigm. For GDPR the cost of compliance is geared to be less than the cost of sanctions.

Tags: john barchie, arrakis consulting, gdpr, general data protection regulation, data security

About John Barchie

John Barchie has twenty years of experience in computer networking, particularly Information Technology and Cyber Security. The majority of his career has been spent developing security protocols for Silicon Valley corporations including Symantec, Paypal, PG&E, KPMG and OpenSky. He has completed security projects for Sony PlayStation and NASA. John is ISACA, (ISC)2 and ISACA certified. For more information, visit www.arrakisconsulting.com.