General Data Protection Regulation (GDPR)

June 2018

Summary

These extensive personal-data protection regulations impact any business that uses the personal data of EU citizens — regardless of where the business is located.

The GDPR applies to all hotels in California.

Failure to comply with the GDPR has stiff penalties. It's important to understand what is required and how to be compliant:

● Update privacy policy and terms and conditions.

● Ensure your web site is secure.

● Ensure cookie consent.

● Ensure the ability to opt-out or erase personal data.

● Update email opt-in to default to "No" and include check boxes for every opt-in.

● State any parties who will receive personal data.

Key GDPR Resources

● How GDPR Privacy Rules Will Impact U.S. Hoteliers

● 2018 GDPR Compliance Checklist for Your Hotel

● A Risk Manager's Guide to the [GDPR]

● GDPR Compliance for Small Business

● Free Excel Assessment Tool

The GDPR (General Data Protection Regulation) seeks to create a data protection law framework across the European Union (EU) and provides EU citizens and their residents control over their personal data, while imposing strict rules on those hosting and processing this data, anywhere in the world. GDPR effective date is May 25, 2018.

Hotels are "Data Controllers"

Since hotel & lodging properties process personal data, they are data controllers and are subject to key obligations and potential liability. Data controllers determine the purposes, conditions and means of processing personal data. Additionally, a company (or person) which processes data for you is also subject to key obligations and potential liability.

Personal Data

In all cases, personal data stored in an IT system, through video surveillance, or on paper is subject to the protection requirements set out in the GDPR. Examples of personal data include:

- Names, email, addresses, date of births, social security numbers, an identification card number, location data (GPS), internet user location, IP address, cookies, RFID tags, advertising identifier (mobile phones), health (HIPAA)/genetic/biometric data, racial and/or ethnic data, political opinions, sexual orientation, union membership

Guest Rights

GDPR introduces enhanced digital rights. Under the GDPR, individuals rights are:

Access – EU citizens or residents can request their personal data, including the right to know if their data is being processed, its whereabouts, and the reason for it. If request, hotels must provide a copy of the personal data, free of charge.

Right to be forgotten – For any reason, an EU citizen or resident can have their personal data deleted or stopped from being processed.

Data portability – Personal data is transferable to another data controller in a commonly used and machine-readable format.

Right to be informed – Consumers must opt in for their data to be gathered, and consent must be freely given rather than implied.

Right to have information corrected – Individuals can have their data updated.

Restrict processing – Individuals can request that their data is not processed.

Right to object – There are no exemptions to this rule, and any processing must stop as soon as a request is received. In addition, this right must be made clear to individuals at the very start of any communication.

Notification – If there has been a breach of personal data, a hotel must inform the individual within 72 hours of first having become aware of the breach.

Explicit Consent

Consent (and withdrawal of consent) must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. Nothing short of "opt in" is acceptable.

Age Requirements

Parental consent is required to process personal data for those under 16 years of age.

Penalties and Liability

Generally, actions seeking relief for violations of the GDPR are brought against data processors and data controllers (e.g., hotels that process/use personal data). There are two remedies for violations – lawsuit from a guest and/or administrative fines.

Individual and Class Action Litigation

- The biggest threat to non-compliant businesses - over and above fines - is risk from individual lawsuits for damages, including class action proceedings.

Fines and Administrative Sanctions

- There is a tiered approach to imposing sanctions on non-complaint controllers and processors. The following sanctions can be imposed:
  - A warning in writing for first and non-intentional noncompliance
  - Regular periodic data protection audits
  - A fine up to €10 million ($16,800,000) or up to 2% of annual revenues, whichever is greater, for not having their records in order, not notifying the supervising authority and data subject about a breach or not conducting impact assessment.
  - A fine up to €20 million ($33,600,000) or up to 4% of annual revenues, whichever is greater, for the most serious infringements, e.g., not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

Business (Hotel) Rights

The "2018 reform of EU data protection rules," provides rules and guidelines to assist businesses and organizations comply with the GDPR.

GDPR and the Hotel Industry

In "How Hotels Should Prepare for the GDPR," it is pointed out that employees and guests are both covered by the GDPR. Hotels need to tell individuals what information is being collected, what it is being used for and how long it will be retained. The GDPR's data protection principles emphasize that organizations should collect data only if it's necessary for a specific purpose and retain it for only as long as it meets that purpose. "Top Concerns Hotels Need to Know About the GDPR and How to Prepare Your Action Plan," notes that one commonly overlooked GDPR regulation is that hotels cannot use profiling to set prices based on an EU visitor's location.

Announcement of Privacy Policy Updates

Email:

We've Updated Our Privacy Policies

To Our Valued Guests:

We're writing to let you know that we've updated our Privacy Policies to ensure that we're fully compliant with the most current data protection requirements.

There is no need for you to take any action at this time. We simply wanted to notify you about our updated Privacy and Cookies Policies for all our websites and to reiterate our commitment to putting you in control of your personal data.

Should you have any questions regarding our updated Privacy Policies, please email us at_____.

Website:

Our Privacy Policy and User Agreement have changed.
By using or registering on any portion of this site, you agree to our updated User Agreement and Privacy Policy and Cookie Statement.

California Hotel & Lodging Association
414 29th | Street Sacramento, CA 95816
(916) 444-5780 | service@calodging.com
www.calodging.com

CH&LA and CABBI members with questions or concerns about GDPR should contact our Member Legal Advisor, Jim Abrams at jim@calodging.com