Crowe Horwath

75 years 1941 · 2016

Smart decisions.
Lasting value.

The impact of GDPR on the hotel sector

GDPR and the hotel sector

When it comes to data security, there are few sectors as vulnerable to threats as the hotel industry. With the volume of processed personal and credit card information being handed over to hotels on a daily basis the hotel industry is currently one of the most vulnerable to data breaches (Verizon 2016 Data Breach Investigations). It is no surprise that the industry accounted for the second largest share of security breaches in 2016.

With the enforcement deadline for the GDPR looming closer, it is imperative that hotels upgrade their data protection processes, or they face the risk of large financial penalties.

The penalties for not complying with GDPR are large, at a financial cost of up to €20 million or 4 per cent of worldwide annual turnover (whichever is greater), not to mention the potential reputational cost to a business in the hospitality industry. However, these possible losses can be avoided if the hotel leaves enough time to efficiently adapt to the regulation.

What is GDPR?

GDPR is a regulation to strengthen and unify data protection for individuals within the European Union. It was adopted in May 2016 and following a two-year implementation period will come into force on May 25th 2018. The legislation brings in a large number of changes, meaning that the level of effort involved in preparing for GDPR compliance is significant.

Capturing and using personal data

Personal data must be collected for specified explicit and legitimate purposes. Data cannot be further processed in a conflicting manner with the purposes outlined initially – for example, taking an email address at the time of booking and then using it, without further consent for email marketing at a later stage. The hotel must ensure customers are aware of the particular uses of their data. Hotels must develop a strategy to obtain consent in appropriate form through communications that are legal prior to the new regulations taking effect.

Hotels accepting credit card payments must already be compliant with the Payment Card Industry Data Security Standard (PCI DSS). This outlines that if a company intends to accept card payment, and store, process and transmit cardholder data, they need to host their data securely with a PCI compliant hosting provider.

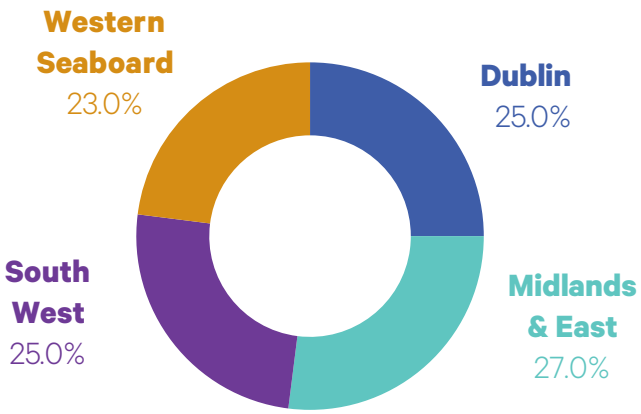
Repeat business and email marketing

With the majority of hotels relying on emails as one of their main forms of marketing, the introduction of GDPR may have a significant impact on their marketing strategy. This regulation states that customers will now have to "opt-in" to an email marketing service, as opposed to the current widely-used "opt-out" system.

Hotels must be able to prove that their customers have given consent for their data to be used for marketing purposes, and must also specify which data they wish to be used. If a list of potential customers has been purchased, the hotelier must also receive documentation that proves that consent from these customers has been given for the data to be used.

Promotional marketing to a customer database is important in the Irish hotel business, particularly given that as many as one in four guests are repeat, as shown in the graph below, from the 2017 Crowe Horwath Annual Ireland Hotel Industry Survey.

Repeat Business by Region 2016



Change to right of access to personal data under GDPR

Under existing Data Protection Acts any individual can write to a hotel and request personal information for a fee of €6.35 and the onus is on the hotel to furnish this data within 40 days. This personal data can relate to both electronic and physical forms and would identify an individual by their personal information such as name, address, dietary preference, medical conditions, etc. Personal information is held across virtually all hotel departments, for example, sales and marketing, reservations, food and beverage, leisure centre and spa.

In the run up to the effective date in May 2018 the Data Commissioner's Office will be running a public awareness campaign about a consumer's 'Right to Seek' their personal data. As a result of that campaign, and because under GDPR the 'Right to Seek' will now be free of charge, we anticipate there will be an increase in consumers requesting their personal data. Also, under the new regulation a hotel will need to comply within the shorter period of 30 days or be subject to a breach of the regulation.

Third party partners

Hoteliers should become more wary of their third-party partners, as they can often prove to be a business's vulnerable point in terms of data protection. A major change due to GDPR is that data processors are captured by the regulations as well as data controllers. This means that if a hotel, as a data controller, is outsourcing the process of data to a third party who is not complying with GDPR regulations, the hotel and the third party processor can be held jointly responsible if a breach occurs.

Preparing for GDPR

It is essential that hotels create awareness and full buy-in from all the hotel management team. There may be changes in procedures or systems, so all managers should be aware of GDPR, fully understand it, and be able to understand the impact on their department. Adequate resources should be set aside to update existing policies and procedures to ensure compliance and staff should have appropriate training for the ongoing maintenance of GDPR compliance. Hotels should also ensure they have an up-to-date PCI certificate.

It is important that hotels devise and implement a plan now to ensure compliance with GDPR before its introduction in May 2018. Below is a 5 step plan to GDPR compliance.

Step 1 – Data mapping

One of the first issues a hotel needs to tackle is that of data discovery. Hotels receive personal data details through multiple channels and touchpoints including email, fax, phone, website, forms, etc., and this data is often stored on multiple platforms across several departments. For example, the front desk will keep details about a guest such as email, telephone, previous visits, room preference and so on; the restaurant might have dietary information; and the spa will have forms for a guest to fill out their medical information. Hotels will need to complete a data mapping process to become aware of what data is captured, where this information is stored, and how it is used before it can begin the process of how to protect and monitor it moving forward.

Step 2 – IT and security assessment

Once a hotel has mapped the data it captures and created a data register, they will need to test and document how secure the data is and identify any weaknesses. The hotel's hardware and software applications should be reviewed along with hard copy files. A series of encryption codes, passwords or limitations on access may need to be implemented to protect access to, and the integrity of the data.

Step 3 – Update GDPR policies and appoint data protection officer

Hotels will need to review all current data protection policies such as their privacy policy, SARs (subject access request) policy, retention policy and other policies like shredding and breach management policy. Their policies relating to third party data contractors should be reviewed and consideration given to the appointment of a data protection officer (DPO).

Step 4 – Implementation of new GDPR policies

The onerous task of cleaning up your current data records should begin – deleting what is not required and validating the data that is required. Begin the process of reaching out to customers to inform them of the new policies and to verify their data and its uses. Document all standard operating procedures (SOPs) and invest in training of all relevant staff members to ensure they have a thorough understanding of the new procedures and the implications of the regulation.

Step 5 – Ongoing compliance and monitoring

Maintaining GDPR awareness with staff is an ongoing process. Hotels should provide regular refresher training for all staff to ensure an awareness culture exists to protect against possible breaches. Management should incorporate data privacy into operational training such as induction, HR and security, and conduct regular access request drills to ensure efficiency with 'Right to Seek' requests.

Next steps

It is important that hoteliers act now to fully access the true impact of the new regulations. The GDPR team at Crowe Horwath can help hoteliers devise and implement a plan to ensure compliance in advance of the May 2018 deadline. If you would like to find out more about how we can help you contact Roseanna O'Hanlon or Simone Kennedy of our risk consulting team.

About Us

Established in 1941, Crowe Horwath is a leading accountancy and business advisory firm in Ireland. Throughout our 75-year history, we have developed an unrivalled understanding of the Irish business environment and built a national reputation in auditing, tax and business consultancy.

We work with a variety of clients across commercial and public sectors. Our services include Audit & Assurance, Tax, Corporate Insolvency & Recovery, Corporate Finance, Consultancy, and Outsourcing.

We are also independent members of the eighth-largest accountancy network in the world, with colleagues in over 750 offices across 130 countries. Through this global reach we are able to offer clients a seamless service when trading internationally.

Our success is the result of our exceptional client service. Together with our clients, we work to optimise the present and maximise the future, tirelessly exploring all possibilities until we find the right solution. We help clients make smarter decisions today that create lasting value for tomorrow.

Smart decisions. Lasting value.

Contact

Crowe Horwath Bastow Charleton
Marine House
Clanwilliam Place
Dublin 2

Tel: +353 1 448 2200
www.crowehorwath.ie

Roseanna O'Hanlon, Partner
roseanna.ohanlon@crowehorwath.ie

Simone Kennedy, Internal Audit
simone.kennedy@crowehorwath.ie