techtalk.travel

Peter Hense

Partner at Spirit Legal LLP

GDPR Compliancy

An update to Data Protection in the Hotel Industry

The honeymoon's over

Data protection management in the hotel industry

Around 500 days have passed since Europe's data protection overhaul became a reality. With its draconian threats of penalties, the General Data Protection Regulation (GDPR) has shaken up companies left, right, and centre. While public authorities announced spot checks on certain core aspects for 2019, consumer organisations are taking legal action against online surveillance tools and hotel chains have begun carefully scrutinising the mass collection of data by third-party portals. To make matters worse, the Payment Services Directive 2 (PSD2), which came into force in September 2019, imposes new Europe-wide rules for electronic payments.

Attorney-at-law Peter Hense explains where hoteliers need to be particularly careful – and how the market has changed.

1. REGULATORY CHECKS

2019 will see a huge spike in regulatory checks and audits in the hotel industry. Germany's data protection authorities alone employ some 650 people to process data protection complaints and notifications. Despite the substantial backlog, companies can expect their past sins – cases from recent years – to come back and haunt them in the form of official proceedings, even if it may take some time. If you haven't received any post yet, that doesn't mean to say that none is coming. The mills of justice grind slowly, but they grind small.

When it comes to the hotel industry, the data protection authorities – and customer complaints – focus on 1) email marketing and messaging; 2) video surveillance; 3) data breach notifications; and 4) web analytics and cookies. In all these areas, we have already handled a considerable number of cases in the past year, gaining a great deal of experience in dealing with customer complaints and privacy litigation.

2. DATA PROTECTION MANAGEMENT, TRAVEL TECHNOLOGY AND DATA MAPPING

The hotel industry is not exactly a driver of innovation. Many systems used in the areas of PMS, CRS, GDS, CRM and IBE were introduced decades ago and struggle to keep pace with the state of the art in other industries. Not convinced? Just compare online fashion, technology or luxury goods retailers with hotel websites. But even legacy IT systems and processes need to be documented and controlled. Every hotel also needs to know who processes which data in the company, when and where this happens, as well as which third-party providers are involved.

At the heart of any data protection management system is therefore 'data mapping', i.e. creating an inventory of all situations where personal data is processed. On the basis of this data mapping, the hotel can document its essential processing operations in so-called records of processing activities (ROPA), and by doing so also satisfy important GDPR provisions on accountability.

3. RISK MANAGEMENT

Instead of splashing out on management consultants, we advise hotels to do one simple team activity: draw up a risk matrix.

Department by department, the matrix is used to propose, discuss and classify potential risks with each and every team member (bottom-up). Sources of risk may include customers, employees and service providers. This risk matrix can then be checked by data protection experts, serving as the basis for a catalogue of measures to be dealt with in order of importance and urgency.

The value of involving your employees in data protection management cannot be overstated: indeed, many data breaches are caused by ignorance of the problem, a failure to appoint contact persons, and incorrect reporting processes within the company. Here it makes sense to rehearse certain crisis scenarios with your employees, such as a data breach, various types of customer complaint, and an official audit.

Evaluating stress tests like these with the teams involved is more valuable than any piece of paper signed by external consultants. But even the best training is useless if it is not repeated. A substantial aspect of risk management under the GDPR is regularly training the relevant personnel – and repeating the necessary stress tests at least annually. When it comes to the GDPR, the costs of compliance pale in comparison to the costs of non-compliance.

4. TIME TO CHECK THOSE CONTRACTS

Hoteliers should review any contracts now which may not have been adjusted in the heat of the moment back in May 2018. According to Article 28 of the GDPR, the (data) controller is obliged to clearly and unambiguously contractually regulate the details of any data processing with processors or joint controllers.

Since the GDPR came into force, it has been possible to do all of this electronically at the click of a mouse. Nevertheless, experience has shown that in the past many such contracts were still concluded on paper – and sometimes whilst quite naively ignoring some of the more important legal nitty-gritty. Unfortunately, these contracts occasionally still contain surprising liability clauses, which a prudent business person would never agree to upon closer examination.

5. EXERCISE CAUTION WITH LABOUR LAW

Entrepreneurs should also check their data processing for weak points with regard to employee data, because data protection and labour law go hand in hand. It is not uncommon for disgruntled workers who have been made redundant to throw data breaches into the equation in their efforts to secure more favourable severance packages.

Hardly a day goes by when courts do not hear cases of alleged or actual breaches of data protection by employers. In order to avoid costly labour disputes due to privacy-related problems, hoteliers should therefore examine the whole gamut of data processing involving their employees and make sure there are no potential weaknesses – from the application process and getting staff to sign confidentiality agreements, to software user permission concepts and even staff photographs.

6. SALES PARTNERS, OTAs AND SERVICE PROVIDERS

Dealing with service providers and sales partners can be frustrating enough for the hotel industry, even without data protection concerns. There's rate parity, availability, brand bidding – and now also external portals and their thirst for data. Booking.com in particular now shares hotel guest data with all affiliated partner companies worldwide, without adequately informing those guests, let alone obtaining their consent. And thanks to the clear provisions of the GDPR, can you guess who's liable for such data breaches by sales partners? That's right: the hotel. Anyone keen to avoid liability risks when dealing with portals should therefore review, update and, if necessary, insure their agreements with these platforms accordingly.

7. COOKIES AND MARKETING

A steady stream of court decisions means that the topic of cookies and web analysis is forever in a state of flux. By late 2019, one thing is clear: web analysis, remarketing and programmatic advertising on hotel websites require the express consent of the user. Website visitors must be told exactly what is done with their data, who receives the data and when it will be erased.

This poses major challenges for the entire online marketing industry, because even with the likes of Google Analytics, the Facebook Pixel and other widespread technologies, it is nigh on impossible to provide the information required by law about how cookies work, storage periods, and data recipients.

The ball is in the court of technology companies, who have quite simply been asleep at the wheel. Even so, hotels can't wash their hands of responsibility; if you know that a technology is not legally compliant, then you must make do without that technology – or use a legally compliant alternative.

It is clear that the authorities mean business: a few days ago in Spain, for example, the airline Vueling was dealt a hefty fine and a usage ban by the authorities because its website used an insufficient cookie banner and stored advertising cookies without the informed consent of users.

8. THE FAIRY TALE OF LEGITIMATE INTERESTS

In 2018, inventive consultants came up with all sorts of nonsense on the subject of 'legitimate interests' – unfortunately, this article is too short to list even the most ludicrous pieces of advice offered.

Under the GDPR, the principle of legitimate interests means that data processing is allowed if the interests of the company – the hotel – are weighed up against those of the data subject – usually the guest – and deemed more important. This balancing of interests is a complicated process and has to be documented in a 'legitimate interests assessment' (LIA) for each data processing operation.

The law allows data processing if three cumulative conditions are met: a) a legitimate interest of the hotel protected by the legal system, e.g. advertising; b) the necessity of processing personal data to achieve the legitimate interest (a point which fails if there are other, less data-intensive ways to achieve the legitimate interest); and c) no overriding fundamental rights and freedoms of the data subject.

Many a marketing dream has been dashed by the fact that it is already impossible to fulfil legal information requirements towards guests, which means that an otherwise legitimate interest in 'marketing' cannot apply. If the hotel cannot correctly inform its guests – about the use of cookies, analysis tools and pixels, about the processing of their data in the CRM, about disclosure to OTAs – then invoking 'legitimate interests' will already fail for this reason. The whole process has to be clean and compliant before this legal basis can come into effect.

9. IMPACT OF A NO-DEAL BREXIT ON THE HOTEL INDUSTRY

Everyone agrees that the effects of Brexit, worse still a no-deal Brexit, would be catastrophic not just in terms of data protection law. For example: a British hotel chain that operates hotels in the EU, collecting guest data there and recording it in a central reservation database, would no longer be allowed to transfer that data company-wide post-Brexit.

Additional mechanisms would be needed to secure this transfer of data to what would then be an insecure third country. In addition to agreeing and implementing Standard Contractual Clauses (SCC) of the EU Commission, this would also include additional consent of the guests, because guests in a French hotel run by a French subsidiary could not be forced to have their data transferred against their will to a reservation system hosted in the UK.

10. FINALLY: PSD2 SPELLS TROUBLE IN PARADISE

The new regulations on strong customer authentication (SCA) pose great challenges for hotel operators in particular. SCA is also required for payments to and from third countries outside the European Union, if the hotel's payment service provider is located within the EU and the payment amount is credited to one of its clearing accounts.

For example, the European payment service provider used by a Caribbean hotel may have to perform SCA for electronic payment transactions.

Tried-and-tested payment structures and processes will no longer be possible in their current form. This applies above all to no-show fees and incidental charges: until now, hotels were able to block funds on a credit card – details of which the customer would provide when booking – in order to debit the blocked amount, or a contractually agreed fee.

Now, blocking a certain amount also requires the explicit consent of the guest pursuant to Article 75(1) of the PSD2. On the other hand, as of 14 September 2019, debiting credit cards in this way is only possible if the payment process has been triggered in accordance with SCA – which the hotel cannot carry out without the payer.

There are a few exceptions, for instance in the case of small amounts of up to 50 euros or if no more than five consecutive payments are triggered without SCA. In most cases though, a no-show charge will significantly exceed the authentication limit. The hotel industry is going to have to rethink how it deals with these charges. One solution could be to ask guests to pay the full price at the time of booking – which may well discourage many of them from booking in the first place.

ABOUT THE AUTHOR

Peter Hense

twitter.com/peterhense

Peter Hense is an attorney-at-law and partner at Spirit Legal LLP, where he heads a team of 15 colleagues working in technology, data and media law, most of whom are women.

An expert in technology law, he specialises in advising clients on international IT and technology law, data usage law and privacy litigation, in particular in the areas of travel technology, distribution, media and competition.