GDPR:REPORT
ALL THE LATEST NEWS AND COMMENT ON GDPR

GDPR – what will it mean for the travel industry – and can you believe everything you read?

2ND JANUARY 2017 BY GDPR REPORT IN FEATURES

Rightly or wrongly, there have been a lot of sensational headlines about GDPR. As we approach May next year, industry commentators and pundits are increasingly offering their take on what GDPR means.

Yes, the latest wave of regulation, in the form of General Data Protection Regulation (GDPR) – the new European-wide legislation – is arriving soon. In fact, it's already law, but will be enforced from 25th May 2018 and replaces the outdated EU regulation enforced via the Data Protection Act 1998.

So let's take stock of what GDPR really means for travel businesses – and whether or not they'll come out a winner or a loser in the shake-up. Because data, as we all know, is the lifeblood of most travel and hospitality companies. In particular online travel agencies – which have as their beating hearts booking engines or CRM systems connected to multiple APIs, databases, suppliers, channel managers and other third-party technology suppliers or partners.

I attended a fascinating forum on GDPR run by the Travel Technology Initiative (TTI) last month, where Nick Towers, managing director of digital agency Sagittarius, revealed that one client, a large UK charity, carried out a third-party audit of their marketing department,

and discovered it was using 32 different digital technologies, collecting or processing data. The list can be endless. The same is true for countless travel sector companies.

Travel and hospitality organisations will have to sit up and take notice of any new regulations that directly affect their data. Some may argue that the imminent introduction of GDPR is good timing, as several companies have fallen foul of hacks, highlighting our fragmented sector's vulnerability to data breaches. Hotels, so reliant on holding debit or credit card details, have been targeted. In April the Holiday Inn chain, owned by InterContinental Hotel Group, suffered a payment card-stealing malware attack at 1,200 of its properties. In July, Sabre's SynXis system was compromised. Meanwhile, in March Abta experienced a data breach with 43,000 individuals affected after a web server hack.

Grabbing the headlines

There has been a certain level of scaremongering taking place with sensational headlines vying for eyeballs, so it was reassuring to see the ICO (Information Commissioner's Office) set the record straight on several issues on its blog these past weeks, mostly relating to fines and reporting. For one, this means the industry can get on with focusing on the technical issues that matter: data documentation, management and security – among other areas handily listed by the ICO here:

The ICO has the authority to impose fines of £17 million or 4% of turnover allowed under GDPR. Many articles have stated GDPR will therefore automatically cripple any company found guilty of a breach. However, UK Information Commissioner Elizabeth Denham says these are the maximum fines and would only be imposed on companies that are repeat offenders, that don't play fair by the new rules. At the TTI forum, technology lawyer Dai Davis said noted the ICO fined only 13 companies last year, with an average fine of £100,000. Data security breaches were reported by 1,950 organisations.

We've also seen headlines stating that all data breaches must be reported to the ICO. That's not strictly true. As Denham states, only those personal data breaches that are likely to result in a risk to people's rights and freedoms must be reported. And individuals need only be contacted if this is the case too – examples include discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage. As she says: "Tell it all, tell it fast, tell the truth" – and you'll be fine.

Perceptions and reactions

One view is that GDPR is government payback time – that it provides a way to finally exert greater control over the giants like Amazon, Facebook and others that have come to dominate our lives. I would disagree: many people are rightly concerned at how their data is being processed for marketing activities and GDPR is based on the principle of returning the control of personal data to the individual, while the Data Protection Bill proposes that we: "make it easier and free for individuals to require an organisation to disclose the personal data it holds on them".

As well as payback, there are suggestions GDPR is another Y2K for some technology consultancies. In the build-up to the year 2000, the Millennium Bug was both big news and big business as the fear factor took hold that computer networks around the world would all crash. Yet since the Data Protection Act 1998, cloud computing and social networks have developed at a pace that back then would have barely been imaginable, and the many major global hacks we have seen recently take advantage of these modern technologies and trends.

Maybe the GDPR headlines are sensational for a reason, sparking debate, and spurring our industry into action. Whatever the reason, the key is to act now. GDPR is complex, so

prepare to document how you will manage and protect your data. Lack of preparation could lead to non-compliance, and while an initial ICO fine might not be high, your reputation will suffer. And in travel today, your brand is everything. By justifying how you capture and use data, and prove compliance, that 25 May 2018 might just be a day you actually look forward to – despite what you read in the meantime.

By Charlotte Lamp Davies, Vice President, Travel & Hospitality DataArt UK

Original article can be found here: https://gdpr.report/news/2017/01/02/gdpr-will-mean-travel-industry-can-believe-everything-read/