

## **Travel Weekly Opinion post**

### **GDPR friend or foe to the agent?**

Winning and retaining customers for agents is hard work and costs money! So when suppliers want to process bookings and take payments directly it's not surprising that agents are reluctant to pass on customer details as they assume, perhaps rightly, those customer details will be hoovered up into a supplier's direct marketing machine as soon as they hit the inbox. And with the prevalence of suppliers looking to take payment directly from customers one might speculate that this is one of their intentions.

There is no doubt the travel industry is challenged in this area, the need to share details of the traveller for identification at the point of service delivery is clear, but as customer acquisition costs rise, agents doing the work at the sharp end to generate new business need to retain those new customers.

Could GDPR be an unexpected knight in shining armour for agents? By the time we are all strolling the aisles of TTE2018 there will be less than 100 days to go until GDPR becomes enforceable by which time all businesses are required to be GDPR compliant. GDPR brings additional data protection obligations that could assist agents to better protect themselves and customers alike.

GDPR makes data controllers and data processors equally responsible for data protection increasing the responsibility of the supplier to be rigorous in their protection of an agent's customer's data. Data processors are only entitled to process data for the purpose that was originally intended, which will have been defined by the agent - so as an example, if payment is taken directly from a customer the supplier should not use the data for marketing - failure to respect this would be a breach of GDPR. This should afford agents some additional protection, assuming they have been clear in their supplier contracts.

An agent needs to update privacy notices and define the lawful basis for processing of customers' data to be certain they are GDPR compliant in this area. They should also ensure that their contracts with suppliers are very clear on the purpose for which the personal data is being processed and what can/can't be done with that data. This may be tough for agents if the supplier is the more powerful party but the protection would be worth the negotiation effort. Being a non-EU supplier doesn't excuse a supplier from compliance either, as the GDPR reach extends to non-EU suppliers when processing the data of EU citizens

There is much talk on the topic of consent. Firstly, agents should understand that consent isn't the only basis for lawful processing however if that is the basis being used it needs to be unambiguous for each use case, plus a record of consent must be maintained. When an agent collects the data from a customer they need to make sure they have been clear with the customer on all intended uses of that data and make it equally easy for a customer to withdraw that consent. Clarity on whether

data is passed to third parties, as part of the consent process will be critical, then ensuring that suppliers respect that consent.

Having got the traveler's details a supplier could use legitimate interest as a basis for communicating with the traveler. Sending them relevant upsell information along with a ticket or confirmation voucher would be acceptable as long as it wasn't refused as part of the consent process but it is starting to stretch the definition of lawful purpose - if the traveler starts to receive regular adhoc marketing blasts for which consent wasn't gathered – then that would most likely be a breach.

We also need the traveler to be more assertive. With all the publicity surrounding GDPR it is likely that rate of unsubscribes to irrelevant marketing blasts increases, but maybe the traveler should go one better and make sure they tick the "I never signed up" button rather than the "I no longer wish to receive" button. Modified behaviour from the traveler will encourage agents and suppliers alike to be conscious of their data protection obligations.

The upshot of the complex GDPR landscape could mean that good governance on the part of the agent may enable them to derive business benefits from GDPR compliance.

Jackie Groves  
Xcelerate Solutions  
January 2018