Get ready for GDPR – how Europe's new data protection legislation affects your travel programme

The EU's General Data Protection Regulation will have a profound impact on corporate travel from May 2018, so it is essential to prepare now. Here are the major issues to think about.

Why GDPR matters to your travel programme

The General Data Protection Regulation takes effect on 25th May 2018. It requires companies to be much more careful about handling the personal data of European citizens, whether that information relates to customers, employees or anyone else.

Fines for the worst failures in data protection will be up to €20 million or 4 per cent of global turnover, whichever is larger. "The rules follow more or less the same principles as previous EU data protection legislation, but what is new is that they will be policed more and businesses will face higher fines for non-compliance," says Søren Schødt, managing director of TravelpoolEurope. "We must show we have done everything we can."

Personal data can include an individual's contact details or their credit card and banking information, all of which are routinely used in business travel. Companies could be liable for misuse even if the data is mishandled by a contracted vendor instead of themselves. "One of the key principles GDPR puts in place is accountability," Marta Dunphy-Moriel of London law firm Fieldfisher told *Business Travel News* in July 2017. "Travel managers need to know what is happening to their data at every stage. That was previously best practice but it's now a statutory requirement."

What is GDPR?

The regulation covers issues such as how data is secured, how long it is retained, who has access and what they are using the data for. One key intention is that data is only used for the purpose for which it was originally given, unless the individual (technically known

as the "data subject") has consented otherwise. The rules on what is considered acceptable consent have been tightened significantly (see below for more detail).

Another important development is much stronger rights for data subjects not only to inspect what data a business holds about them but to require part or all of that information to be deleted. One way for businesses to think about GDPR is that their database no longer belongs to them; it belongs to the individuals whose data is stored in it.

The "right to be forgotten" is a very good example of why GDPR will be a massive undertaking. Accepting a request to delete a data subject's information is simple in principle but in practice it is very difficult. Their data could be stored on your behalf by service providers around the world, and could also lie in dormant back-up databases which are only restored several years later. The airline Flybe was fined earlier this year for contacting people who had requested removal from its distribution list.

Managed travel has both advantages and disadvantages reagarding data privacy. The good news concerns "sensitive data" – details such as ethnicity, sexual orientation, politics, religion and health – which requires even greater protection than standard personal data. TravelpoolEurope has found only two circumstances where traveller records may contain sensitive data. One is airline meal choices; the other is free-form notes added to a traveller profile which may reveal a health issue – a request for a wheelchair, for example.

The bad news is just how many different parties receive data within the managed travel process: TMCs, airlines, hotels, car rental companies, expense management providers, card companies and booking tools are just a few example. TravelpoolEurope found 17 different kinds of relevant vendor in total. That makes the task of tracking who has your travellers' data and how they treat it extremely complex.

How to prepare your travel programme for GDPR

Audit your data

Build a complete map of your travel data flow as it stands today:

- Which service providers and suppliers hold data on your travellers?
- What personal data do they hold?
- For what purposes do they use the data?
- Is there explicit, implicit or no consent from the data subjects for their data to be used for those purposes (see below)?
- How, if at all, is data protection covered in your service provider and supplier contracts?

Find the right colleagues

You don't have to manage GDPR alone. The regulation requires many companies to appoint a data protection officer, and they can help you. Speak also to your legal, human resources and even procurement teams, which may also have relevant expertise. Share with them all the information you gathered in your audit.

Take mitigating actions

- Prioritise "surprise minimisation": data subjects should never be suprised about who holds their data or how it is being used. If this test fails, delete the data.
- Review and improve data security. Insisting on encryption of all file transfers is a good starting point. Check what your contractors are doing to anticipate GDPR, e.g. training their staff.
- Rewrite contracts to ensure the contractor commits to following all aspects of GDPR. Just two examples are deleting data when notified an employee has left the company, and giving immediate notification of data security breaches. But don't forget, a contract is no longer sufficient mitigation. In future you need to show evidence you are monitoring contractor compliance with GDPR.

Deal with the issue of consent

Consent is one of the most challenging aspects of GDPR and needs careful thought. Consent is required from data subjects if anyone intends to use their data for a different purpose than for the reason it was gathered originally. For example, you don't need a traveller's consent to use data for a booking they have requested, but if a preferred supplier wants to make them a special offer, consent would be needed.

It is also essential to clarify what you are seeking consent for, and to retain evidence that consent was given freely. You cannot require subjects to consent to alternative use of the data as a condition of providing the original service for which the data was submitted.

Consent becomes a particularly difficult question when combined with profiling – for example, an airline or hotel using what it knows about a person to make them a special offer. Profile-based marketing is permitted if consent for that kind of marketing is given, but how that consent can be obtained without performing profiling in the first place is not always clear. This could affect new kinds of personalised services like TMC chatbots, so expect more exploration of this topic.

Manage cross-border data transfer

Under GDPR, companies must take mitigating measures for transfer of information to countries judged to maintain lower data protection standards than the EU (only a handful of countries are considered to have equivalent "adequate" standards). This is a serious matter for corporate travel because much of the sector's data is stored in the US.

A new framework for adequate transfer to the US, called Privacy Shield, has critics on both sides of the Atlantic. A major review of Privacy Shield, which is used by 2,100 US entities, will be carried out by EU data privacy commissioners in September and could determine its future. Meanwhile, an alternative transfer adequacy mechanism called model or standard contractual clauses is under legal challenge. These issues need to be watched closely.

Find out more

This is, inevitably, just a brief introduction to GDPR, and no actions should be taken on the basis of reading this article alone. A useful general guide to the subject is Preparing for the General Data Protection Regulation (GDPR) – 12 steps to take now, published by the UK Information Commissioner's Office.

The TravelpoolEurope perspective – Getting GDPR-ready has been good for us as well as our members

TravelpoolEurope has been working towards GDPR compliance since 2016. Steps taken include:

- Working with our lawyers to create a plan.
- Auditing the suppliers and service providers to which we send personal data of travellers.
- Improving all aspects of data security.
- Addressing consent issues by preparing information for our travel policies and booking tools about how data is used, and asking travellers to approve.
- Making sure all contracts require vendors to be GDPR-compliant.
- Creating standard contractual clauses for data transfers outside the EU.

Overall, getting ready for GDPR has generated extra work, but none of it has been wasted. GDPR turns into law what is good practice anyway. GDPR improves data protection for our members' travellers and reduces the likelihood of mishandling by us or our suppliers and service providers.