

# Cover all data bases

Before the General Data Protection Regulation comes into play from May 25 next year, *Richard Bristow*, Tamite Secure IT director, looks at how travel companies can best prepare

**T**he General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

GDPR is already law. Enforcement will take place from May 25, 2018 - and every business that transacts client data must be compliant by then.

The law is designed to standardise data protection authorities throughout the EU with one standard set of rules. These are based on a single principle - to return control of data held about an individual to the individual. This will require any company doing business within the EU - and with the EU - to comply with GDPR. While it remains in the EU, the UK will be required to comply and will enact it into UK law post-Brexit.

Travel businesses will be particularly hard hit by GDPR as they will need to make significant changes to work practices in order to comply and to protect customers' information (data). This is due to the number of suppliers they deal with and therefore the number of application programme interfaces (APIs) they have from and to their computer systems. They must not only ensure that their own systems are compliant with the new regulation, but also ensure that they fully manage the data controller and data processor relationship. It amounts to a great deal of work - every turn you take often creates more business issues that need to be addressed.

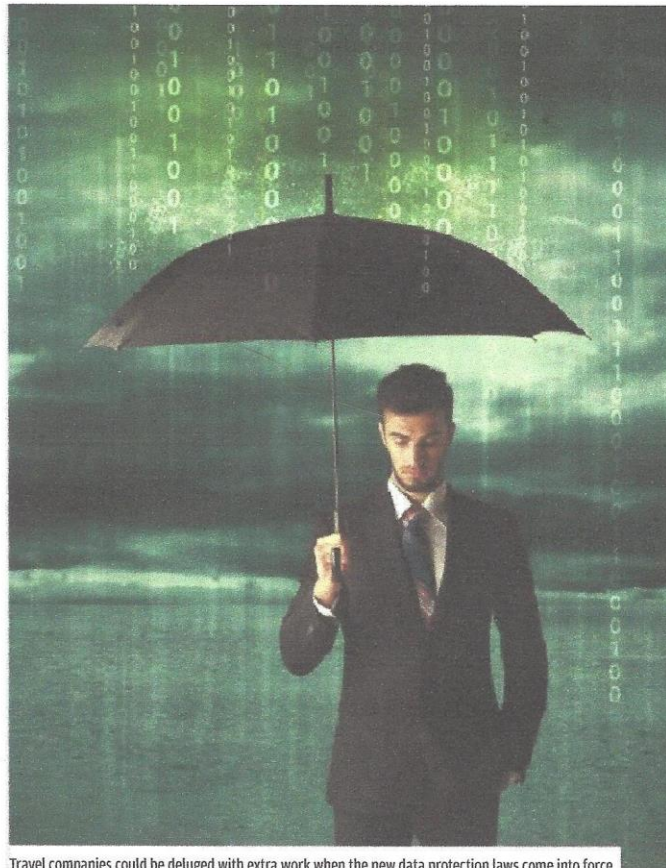
Here are some of the main aspects of the regulation:

## Increased territorial scope

Perhaps the major change is that now there is one single regulation throughout the EU, both pre and post Brexit. It levels the playing field to one single law for 28 countries and will make life simpler in the long term.

## Penalties

The cost of non-compliance is designed to make businesses sit up and take notice. For not getting business records in order and not complying with



Travel companies could be deluged with extra work when the new data protection laws come into force

regulations by having systems assessed, the maximum fine is €10 million or 2% of global turnover. Meanwhile, the maximum fine for data breaches or loss or not meeting privacy design concepts is €20 million and 4% of global turnover. These are maximum fines, but you can count on day-to-day fines being considerably higher than they are today. The message that the EU is putting out there is that "you have to do this".

## Consent

Individuals now own their data and GDPR is designed to protect that information. Companies will no longer be able to hide behind illegible terms and conditions, and websites and business systems must secure individuals' consent at each point of the business relationship and secure their data at all times.

GDPR offers many advantages to businesses both large and small, but the

work required to comply is significant. Major geopolitical blocks need to work together; for example, the EU and the US have the EU-US Privacy Shield agreement in place (which replaces the Safe Harbour deal) that gives businesses breathing space to fully implement GDPR with their own data protection laws and vice versa. Other agreements have been or are being drawn up with Asian, Australian and New Zealand authorities.

GDPR sets minimum standards. Therefore, member states can make their own additions to it. For example, countries such as Germany and Hungary make having a data protection officer a legal requirement where it is only a suggestion for most members.

In summary, it is vital that every company doing business within and with the European Community complies with GDPR by May 25, 2018. Start now, and seek advice. Leaving it too late could result in big financial penalties.