GLOBAL BUSINESS TRAVEL

The General Data Protection Regulation (GDPR): are you ready?

American Express Global Business Travel April 2018

How to prepare your travel programme for changes to data privacy laws

Introduction

When the European Union's General Data Protection Regulation (GDPR) comes into force on 25 May 2018, it will represent the most comprehensive update to global data privacy regulations in decades.

The aim of the GDPR is to ensure businesses are transparent about and accountable for how they handle individuals' information. It touches all aspects of business and has the potential to impose strict sanctions, including fines of up to **€20 million** or 4% of global turnover, whichever is higher.

Businesses that must comply with the new regulation will need to have strict processes in place for how they collect, store and use personal data in the course of their commercial activities. It means businesses must have a clear understanding about where the personal data they collect resides, and how it's used and secured.

Worldwide Impact

One significant change from earlier data protection laws is in the scope of GDPR's extraterritorial reach: Although the rules have been developed by the European Union (EU), other businesses around the world are likely to need to meet the GDPR requirements if they have a presence, offer goods and services or monitor individuals' behaviours in the EU.

Research suggests few businesses are ready for the new regime. According to the *2017 Veritas GDPR Report*, 86% of 900 organizations surveyed around the world were concerned that a failure to adhere to GDPR could have a major negative impact on their business.

PRIVACY BY DESIGN:

American Express Global Business Travel (GBT) is GDPR-ready

Our legacy as part of a bank holding company and our financial compliance and security roots put us in a strong position to meet the GDPR's accountability requirements. Since 2015, American Express GBT has created, conducted and improved the Privacy Risk Management Programme, an accountability framework built for GDPR-readiness.

The Privacy Risk Management Programme operates seamlessly with the American Express GBT data governance programme and an information security risk management framework. Together, these interlocking programmes help ensure comprehensive compliance, including:

- responsible privacy personnel, including a data protection officer
- enterprise privacy and security awareness training
- demonstrable privacy and security compliance testing and reporting
- regular internal audits
- updated privacy notices
- comprehensive data processor risk management, including processing agreements and regular privacy and security risk assessment

Data protection law is about two interrelated concepts:

- What rights does the individual have about their personal data?
- What processes do companies need to put into place to make sure those rights are being respected?

FOCUS ON THE INDIVIDUAL

Under the GDPR, individuals have the right to know what personal data a company has about them. These individuals are referred to as the 'data subjects'. Businesses must tell data subjects why they are collecting their personal data and disclose other details of their data operations that ensure they are acting with transparency.

Data subjects also have the right to make choices about how their information is used. Businesses must, under certain conditions, let individuals consent to or object to processing activities, erase their information, or transfer their data to a new provider – this is known as their 'right to data portability'.

To comply with the GDPR, first it's important to understand what personal data is. It includes things that would traditionally be understood as personal data, like names, passport numbers and dates of birth. But GDPR also clarifies and confirms that personal data includes other information that allows companies to identify, locate, contact or single out an individual, including unique identifiers such as IP addresses or mobile phone identifiers – and the kinds of travel records and locators that predominate in travel services.

How to prepare your GDPR-compliant privacy programme

Data protection law has always required that companies have policies and supporting systems in place to protect personal data and ensure that data subjects can access it. GDPR's most significant change to these requirements is in what's called accountability. It's not enough just to comply with the law; companies must be able to demonstrate that they comply.

When preparing to become compliant with the GDPR, focus on developing a robust accountability framework that allows you to document, measure and communicate your data processes. The building blocks to do that include:

CREATING A DATA INVENTORY

Some data protection laws have historically included a concept called the 'register of processing', which required companies to maintain a written report with the details of all their data processing activities. The GDPR adopts this requirement for all regulated companies.

"It seems obvious, but the first step to making sure all your data-processing activities are lawful is to map out what data you have, where and why," says Kasey Chappelle, American Express GBT's Chief Privacy Officer. "It's not just the law – smart companies will take this as an opportunity to build a data inventory that is essential to good data governance."

TRANSPARENT DATA PROCESSING

Businesses must ensure that they are effectively and transparently communicating their data processing activities to data subjects. That includes having a complete and compliant privacy notice. "A business's privacy notice must be easy to read: concise, transparent and written in clear and plain language, and easily accessible – so that anyone can understand how their data will be used and be able to give meaningful consent where necessary," says Chappelle.

The privacy notice must also describe how personal data may be transferred within the business, to third parties and to other jurisdictions, and how data subjects can exercise their rights.

Transparency doesn't end with a privacy notice. Companies can make sure data subjects understand how their data is used by building 'privacy by design' into their products and services — a concept also now mandated in the GDPR's new obligations of data protection by design and by default.

KEEPING INTERNATIONAL TRANSFERS COMPLIANT

Companies will need to understand the law's strict requirements around international transfers, especially for services like travel that inherently cross borders. EU data must continue to be protected to an EU standard wherever it is stored, accessed or processed anywhere in the world, both within the corporate family or shared with third-party processors.

Companies can achieve compliance through several mechanisms, for example adopting EU-approved Binding Corporate Rules or executing a set of EU Standard Contractual Clauses. First, it's necessary for companies to understand their data flows, then they can ensure that there is a mechanism in place for each.

EFFECTIVELY MANAGING DATA PROTECTION RISK IN THE SUPPLY CHAIN

It's essential for businesses to have confidence that other firms to which they transfer personal data also meet global privacy regulations.

Travel services involve enormously complex data transactions. Each day, personal data such as names and passport numbers goes from the data subject to a variety of third parties. If this information could not be transferred, people would not be able to travel.

Some of the many companies that receive travel data, such as global distribution systems (GDSs), airlines, hotels and other travel suppliers, are recognised by EU regulators as data controllers directly regulated under data protection law. Others are data processors — companies who process data only at the direction of another data controller.

GDPR tightens the rules around how data controllers engage and oversee data processors, and it imposes new direct regulations on data processors too. Companies will only be able to comply when they have robust processes for managing third-party relationships.

American Express GBT works closely with third-party suppliers to assess how they handle personal information and clarify that they understand and are meeting their privacy obligations. "For a travel buyer working with Travel Management Companies (TMCs), they want the assurances that the TMC has not only built data security and privacy into their processes, but has also built it into their vendor on-boarding process," says Chappelle. "Here at American Express GBT, this process incorporates the same privacy risk assessments that our own product development process does — the vendors must share evidence that they have an appropriate privacy programme and the right security protocols in place."

APPOINTING A DATA PROTECTION OFFICER

Under the GDPR, many companies will need to appoint a data protection officer — this person within the business takes on responsibility for the organisation's data protection compliance, and must have the support, resources, tools, knowledge and authority to effectively carry out this role. Some firms will be able to outsource this requirement to a qualified external expert.

EFFECTIVELY TRIAGING DATA BREACHES

Mandatory breach notifications are a major part of EU privacy rules. Under the GDPR, there are two notification requirements if an individual's data is breached. The relevant country's data protection regulator must be notified within 72 hours of becoming aware of the breach. In some cases, the data subject must also be notified.

Triage is a process of categorising issues and prioritising the most critical — in this instance potential and real breaches to privacy laws. Developing a triage-based management system for handling complaints and issues enables businesses to identify and prioritise potential breaches to privacy or security. They need to be able to triage complaints and reports, quickly identify, escalate and remediate a breach, and have mechanisms in place to communicate with regulators and impacted individuals.

"At American Express GBT, we take a multi-tiered approach to identifying issues and managing complaints about privacy or security," says Chappelle. "A phone and online hotline is available at any time to all employees, who can talk to someone in the language of their choice. Every employee complaint is immediately categorised — for instance as a data protection, security or human resources concern, before being appropriately escalated."

CONCLUSION

The GDPR is an opportunity for organisations and their providers to come together to build a shared understanding of these new obligations and ensure the systems and processes that exist between the businesses comply with these new rules. This should include developing systems and procedures to follow when there is a breach.

The idea is to look at personal data protection as a whole-of-business issue, work closely with third parties and vendors, and build in data protection as part of day-to-day operations.

Remember: deadline day for the GDPR is 25 May 2018.

If your business has not yet addressed these issues, now is the time to act. While your travel service providers are 'data controllers', so too are you when it comes to responsibility for your employees' data.

One of your first ports of call should be talking to your TMC, and asking if they have the rigorous data privacy best practices in place to be compliance-ready for the GDPR.

NEED TO KNOW MORE?

Contact American Express GBT at:

https://www.amexglobalbusinesstravel.com/uk/contact

Contactmeuk@amexgbt.com