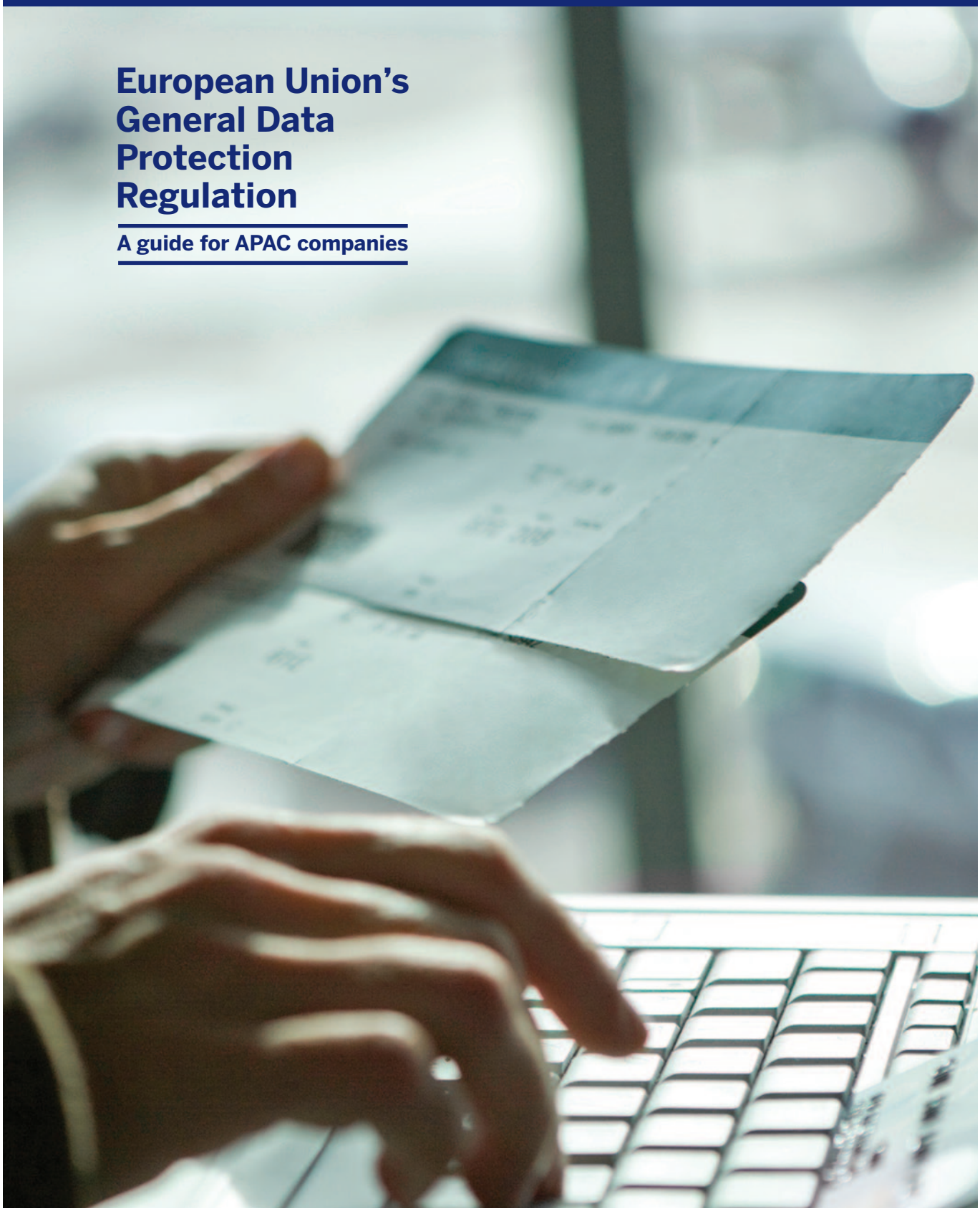
GLOBAL BUSINESS TRAVEL

European Union's General Data Protection Regulation

A guide for APAC companies



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.

These rules address two interrelated concepts, the rights individuals have about their personal data, and processes companies need to put into place to make sure those rights are respected.

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 on businesses. These include fines of up to €20 million or 4% of global turnover, whichever is higher.

As a result of the new rules, businesses need to have strict processes in place for how they collect, store and use personal data in the course of their commercial activities. A necessary precursor to compliance with the law is a clear understanding about where personal data resides and how it's used and secured.

Europe is at the forefront of data privacy regulations and the GDPR harmonises national European rules into the most comprehensive data privacy regulation in the world. The GDPR is much broader and stricter than most, if not all, national data privacy protection regimes.

A view on data protection around APAC

Although the European Union (EU) developed the rules, Asia Pacific businesses are likely to need to meet the GDPR's regulations if they have a presence, offer goods or services or monitor individuals' behaviours in the EU.

Looking across Asia Pacific nations, Japan and the European Union have worked together to prepare a joint statement on the international transfer of personal data. The ultimate aim is to jointly recognise each jurisdiction has adequate levels of personal data protection. This will allow for the standard transfer of data between the two countries without the need for contract clauses, binding rules or privacy certification. Japan's Personal Information Protection Commission oversees the nation's privacy laws.

Hong Kong's laws have been modelled on the EU's privacy laws since 1996, when Hong Kong introduced the Personal Data (Privacy) Ordinance, which came in only a year after the seminal European Data Protection Directive. An amendment was published to Hong Kong's laws in 2012. The laws comprise six protection principles that govern the lawful collection of data. They prohibit excessive collection of personal data and ensure information that is collected is used only for intended purposes. They also allow individuals to access and correct their data.

> "It's not enough to rely on systems to comply with other national privacy laws and assume you will meet European privacy obligations."
>
> Philip Catania,
> Corrs Chambers Westgarth partner.

In Singapore, the Personal Data Protection Act was passed in 2012. Although like the GDPR it has extraterritorial reach, this is a light-touch regime that is not as rigorous as the GDPR. The Singaporean laws apply to the access to, correction and erasure of personal data. The consent provisions are also not as strict as the GDPR's.

Under Australia's Privacy Act 1988, from a private sector perspective the onus is on firms of any size to identify whether and how they are affected by the new rules and put in place measures to ensure they remain compliant.

Australia is one of the nations to be granted 'adequacy' status by the European Commission, which means data can be transferred to the EU without further legal controls.

Across Asia, the APEC Privacy Framework and Cross Border Privacy Rules are intended to apply to countries that don't have a national privacy regime. They provide protection for private information and reduce barriers to information flow between APEC nations.

Now the EU has revised its laws, organisations can expect to see many changes in their local laws. The onus is on businesses of any size to determine if they are affected by the new law and take steps to ensure they comply.

Australia's privacy laws, for example, apply only to businesses with annual turnover of more than $3 million, while Singapore's privacy rules do not apply to the public sector or its agencies. In contrast, the GDPR applies to businesses of any size.

"It's not enough to rely on systems to comply with other national privacy laws and assume you will meet European privacy obligations," says Corrs Chambers Westgarth partner Philip Catania.

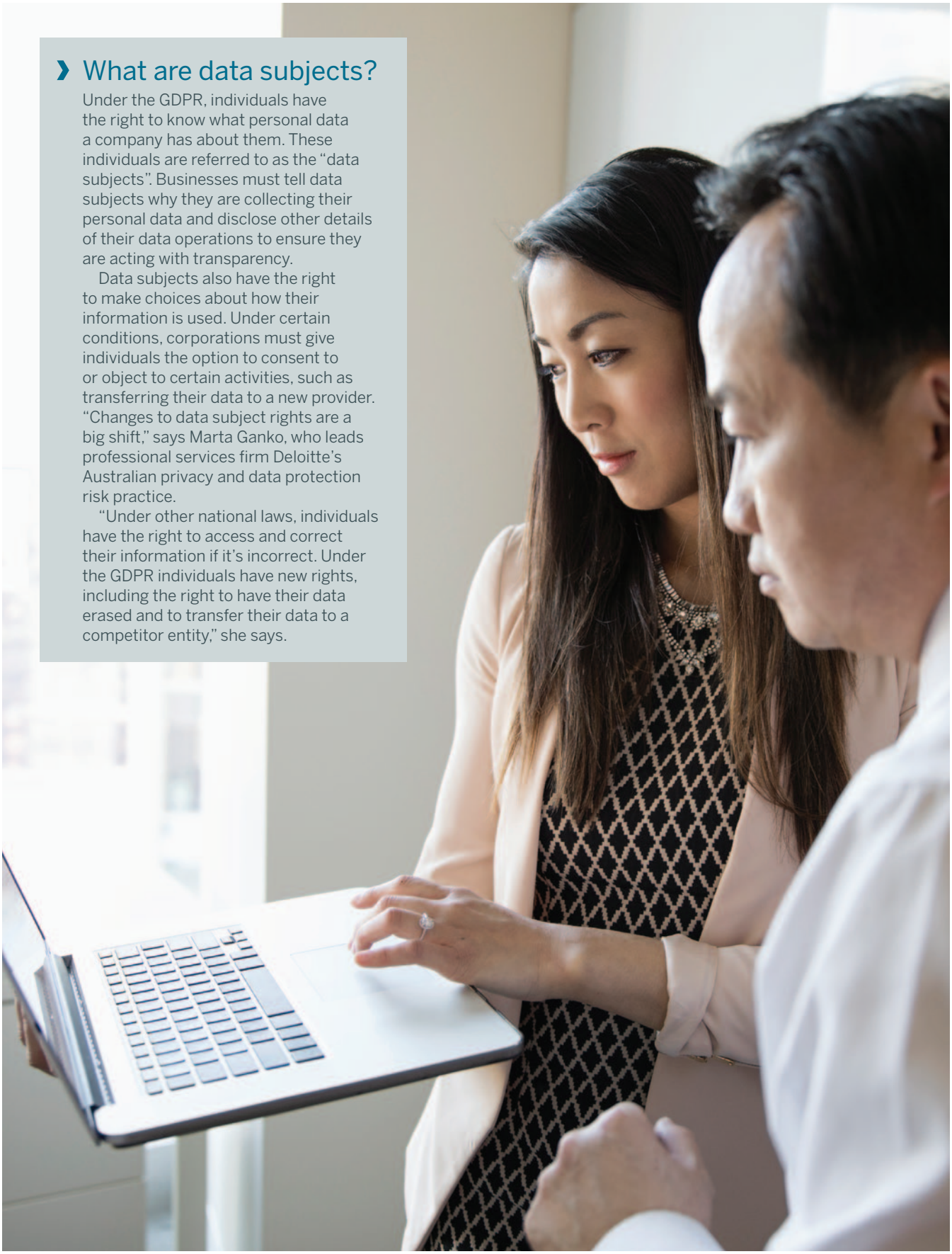
"In Europe, you need consent to collect personal information. So from now on, if you're doing business in Europe, businesses must tell people they are collecting their personal information and ask for their consent," says Catania.

What are data subjects?

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 to ensure they are acting with transparency.

Data subjects also have the right to make choices about how their information is used. Under certain conditions, corporations must give individuals the option to consent to or object to certain activities, such as transferring their data to a new provider. "Changes to data subject rights are a big shift," says Marta Ganko, who leads professional services firm Deloitte's Australian privacy and data protection risk practice.

"Under other national laws, individuals have the right to access and correct their information if it's incorrect. Under the GDPR individuals have new rights, including the right to have their data erased and to transfer their data to a competitor entity," she says.



“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.”

Kasey Chappelle,
American Express GBT chief privacy officer.

How to prepare

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 the GDPR clarifies that personal data also 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, as well as travel records.

The notion of accountability is the most significant change under GDPR. This is the idea that it’s not enough just to comply with the law; companies must be able to prove compliance.

So, when preparing to become compliant with the GDPR, the idea is to focus on developing a robust accountability framework that allows businesses to document, measure and communicate 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.

“The first step to ensuring all data processing activities are lawful is to map out what data you have, where and why,” says Kasey Chappelle, American Express Global Business Travel’s (GBT) 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.”

A complete and accurate data inventory helps an organisation ensure it can meet its GDPR obligations. But experts say businesses are at different states of readiness. “Some are still not able to answer the basic questions: what data are we collecting? Where is this data stored?” says Pelin Nancarrow, Asia Pacific lead, IBM X-Force Incident Response and Intelligence Services.

Ensuring 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 should be easy to read, so the average consumer can understand how their data will be used,” says Sasha Kalb, American Express GBT’s vice president of compliance for the Asia Pacific region. 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. Businesses need to make sure data subjects understand how their data is used by building privacy requirements into their products and services – a concept also now mandated in the GDPR’s new data protection obligations.

Keeping international transfers compliant

Firms will need to understand the GDPR’s strict requirements around international transfers, especially for services like travel that 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 business 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.

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, like global distribution systems, 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 that 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 regulations on data processors. Companies will only be able to comply when they have robust processes for managing third-party relationships.

“At American Express GBT, we communicate our expectations about vendors’ approach to privacy during a risk assessment when they share evidence they have an appropriate privacy program and the right security protocols in place,” says Chappelle.

Focus on the individual

It's important to understand cultural influence to appreciate the difference between Asia Pacific and European approaches to privacy. European data protection laws concern fundamental human rights – data belongs to individuals who have a right to make decisions about how it is used.

"Asia Pacific nations have a more casual approach to privacy," says Brian Fletcher, director of government affairs for Australia-Pacific, Japan and Korea at cyber security firm Symantec. "Europeans take it much more seriously and there's a risk other nations don't take it seriously enough, which could potentially damage businesses in these jurisdictions. Firms could lose business if European partners think they are complacent," he adds.

"It's essential to have risk management processes to be able to assess any risks to which third parties are exposed. These include contractual, physical, legal and regulatory non-compliance risks," says Nancarrow.

Any business with European partners must understand its data protection obligations, especially any contractual obligations they apply to the way personal data is handled. European businesses will require their Asia Pacific partners to put in place new mechanisms to ensure any personal data transferred between them meets the GDPR's requirements.

Appointing a data protection officer

Under the GDPR, many companies will need to appoint a data protection officer with responsibility for overseeing the business's data management systems and for monitoring compliance with the GDPR. Some firms will outsource this requirement to a qualified external expert such as a lawyer.

Effectively triaging data breaches

Mandatory breach notifications are a major part of European 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.

Businesses need to develop a system that lets them identify and prioritise potential breaches to privacy. They need to be able to triage complaints and reports, that is, quickly identify, escalate and remediate a breach, and have mechanisms in place to communicate with regulators and people who are affected by the breach.

"American Express GBT takes a multi-tiered approach to complaints about privacy breaches and issues management. We have a 24/7 hotline any employee can call and speak to someone in the language of their choice," says Kalb. Any complaint submitted by an employee is immediately categorised, for instance as a data protection, security, or human resources concern, before being appropriately escalated.

Breach response obligations require organisations to identify and notify breaches in a timely manner. When a breach comes to light, perhaps during the scrutiny of media reporting, it can have a significant impact on customer trust. Effectively managing privacy and security breaches is more than just a legal issue. The greatest risk is that loss of trust leads to lost business, which could result in significant financial loss.

> "It's essential to have risk management processes to be able to assess any risks to which third parties are exposed. These include contractual, physical, legal and regulatory non-compliance risks."
>
> Pelin Nancarrow,
> Asia Pacific lead, IBM X-Force Incident Response and Intelligence Services.

American Express Global Business Travel is GDPR-ready

Privacy is at the heart of everything American Express Global Business Travel does.

As part of our day-to-day operations, we collect a significant amount of sensitive personal information including names, passport numbers, dates of birth, driver's licence details and dietary and health information.

American Express GBT's legacy as part of a bank holding company and its 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 American Express GBT's data governance programme and an information security risk management framework.

These interlocking programmes include:

- responsible privacy personnel, including a data protection officer
- enterprise privacy and security awareness training
- demonstrable privacy and security compliance testing and reporting
- handling procedures for complaints, inquiries and subject rights requests
- regular internal audits
- updated privacy notices
- comprehensive data processor risk management, including processing agreements and regular privacy and security risk assessment
- incident reporting, response and notification procedures
- privacy and security by design built into our product development lifecycle
- lawful international transfer mechanisms, including the TMC industry's only Binding Corporate Rules.

Conclusion

The GDPR is an opportunity for organisations and their providers 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.

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.

Ultimately, the new rules mean businesses disregard proper personal data protection at their peril.

Need to know more?

Contact American Express Global Business Travel by clicking these icons