Why every APAC financial institution and outsource provider to EU financial institutions should be thinking about GDPR

EY
Building a better working world

What will the General Data Protection Regulation (GDPR) mean for your APAC financial institution – now and in the future?

The GDPR is an EU-wide regulation coming into force from 25 May 2018. It will impose a strict data privacy compliance regime on organizations everywhere in the world that collect, process or if they come into contact with the personal data of individuals residing in the EU. The new regime captures many Asia-Pacific (APAC) institutions that trade directly or indirectly with EU residents and individuals located in the EY, or process EU customer data through indirect secondary relationships with EU financial institutions around Asia that have increasing customer interests in Europe.

To be clear, if your institution offers financial services to, or monitors the behavior of, individuals in the EU – either directly or through indirect relationships – then the GDPR applies to you.

What does GDPR compliance require?

Under the new regime, individuals will hold the right to have their personal data erased if it is no longer needed for its original purpose for collection. At any time, individuals will be able to withdraw their consent for you to hold their data.

Compliance with these strict requirements will take a granular level of control that few APAC companies currently need or have over customer data. It will also require new policies, processes and controls, and, for many organizations, the introduction of a new mandatory senior and independent role: the data protection officer (DPO).

To avoid incurring major fines, organizations must demonstrate that they are accountable for protecting and respecting their customers' and employees' personal data (e.g., GDPR brings in significant changes that go beyond the requirements of most APAC data protection regulations). Organizations may find they need to rethink and redesign their current privacy practices to become GDPR-compliant.

These changes include:

- **Accountability:** The GDPR increases the accountability of organizations entrusted with processing and managing personal information. Organizations will be required to demonstrate their compliance, which includes documenting data and processing activities, completing privacy impact assessments, and performing regular privacy audits and policy reviews. This will be a significant change for most APAC organizations.
- **Right to erasure:** APAC organizations affected by the GDPR will have to facilitate the means for individuals to exercise their right to erasure of personal data. This means, where certain conditions are satisfied, on an individual's request, organizations must be able to identify where that person's data is located and then ensure it is erased completely of all systems. This is no easy task given how far and wide data is spread across organizations, countries and third-party data processors.
- **Mandatory data breach notifications:** Data breaches that could result in a risk to an individual's privacy rights must be notified to supervisory authorities within 72 hours. In some cases, breaches must also be notified to all of the individuals impacted. For most APAC organizations, compliance with mandatory data breach notification will require significant new policies and processes.
- **Consent:** GDPR introduces more stringent consent requirements, including:
  - The consent must be active — an individual simply taking no action (i.e., not unticking acknowledgement box) will not be considered as providing consent.
  - Separate consents are required for each different processing activity — they cannot be bundled together.
  - Supply of services cannot be made contingent on an individual consenting to processing that is not necessary for the service being supplied.
  - Individuals must be clearly informed of their right to withdraw their consent.
- **DPO:** Many organizations subject to GDPR will need to appoint a DPO, whose primary objective will be to oversee and manage data privacy, ensure GDPR compliance, and liaise with authorities and individuals. The DPO must report directly to the highest level of management in the organization.

The scale and size of an organization's operations will add complexity to how they must organize their collection, processing, storage and retention of data. APAC organizations subject to GDPR must find a way to meet these very challenging requirements in a balanced and risk-focused way.

Preparedness across Europe

In Europe, the pending enforcement has been accompanied by a rare level of alert and preparedness among business for a very good reason — the GDPR comes with severe fines.

Those failing to comply with the new regime will be liable for penalties of up to 4% of their worldwide corporate turnover or €20million, whichever is greater.

These penalties apply not only to a data breach but also to a wide range of infringements, including basic procedural contraventions.

APAC challenges and what you should expect

While many APAC countries have some privacy and data protection regulations, they are lagging behind the current new wave of related reforms championed by the GDPR. For those not covering GDPR, it may seem that the buzz around privacy isn't a local issue, but APAC regulations are expected to evolve and rise to GDPR standards as international regulations become more standardized and the GDPR is considered the new norm. This means that even organizations not currently caught by GDPR and based in APAC or operating in countries without robust data protection laws must be prepared for inevitable change. Already, Australia has introduced new mandatory breach notification requirements and stricter penalties, and New Zealand is expected to soon follow suit.

In the long term, harmonization of privacy laws across APAC will eventually make business easier for multinational companies. In the short term, however, it puts pressure not only on business-as-usual operations and budgets but especially on the larger digital transformation programs that rely on both a wide use of data and free flow as well.

Benefits beyond compliance

On the upside, GDPR offers the financial services sector a good baseline of privacy and data management controls that every APAC financial institution should consider adhering to in any event. It establishes a set of standards and practices which, if implemented appropriately, should appease and prevent the public's key privacy fears. With the increasing number of data breaches making headlines, individuals are searching for institutions they can trust.

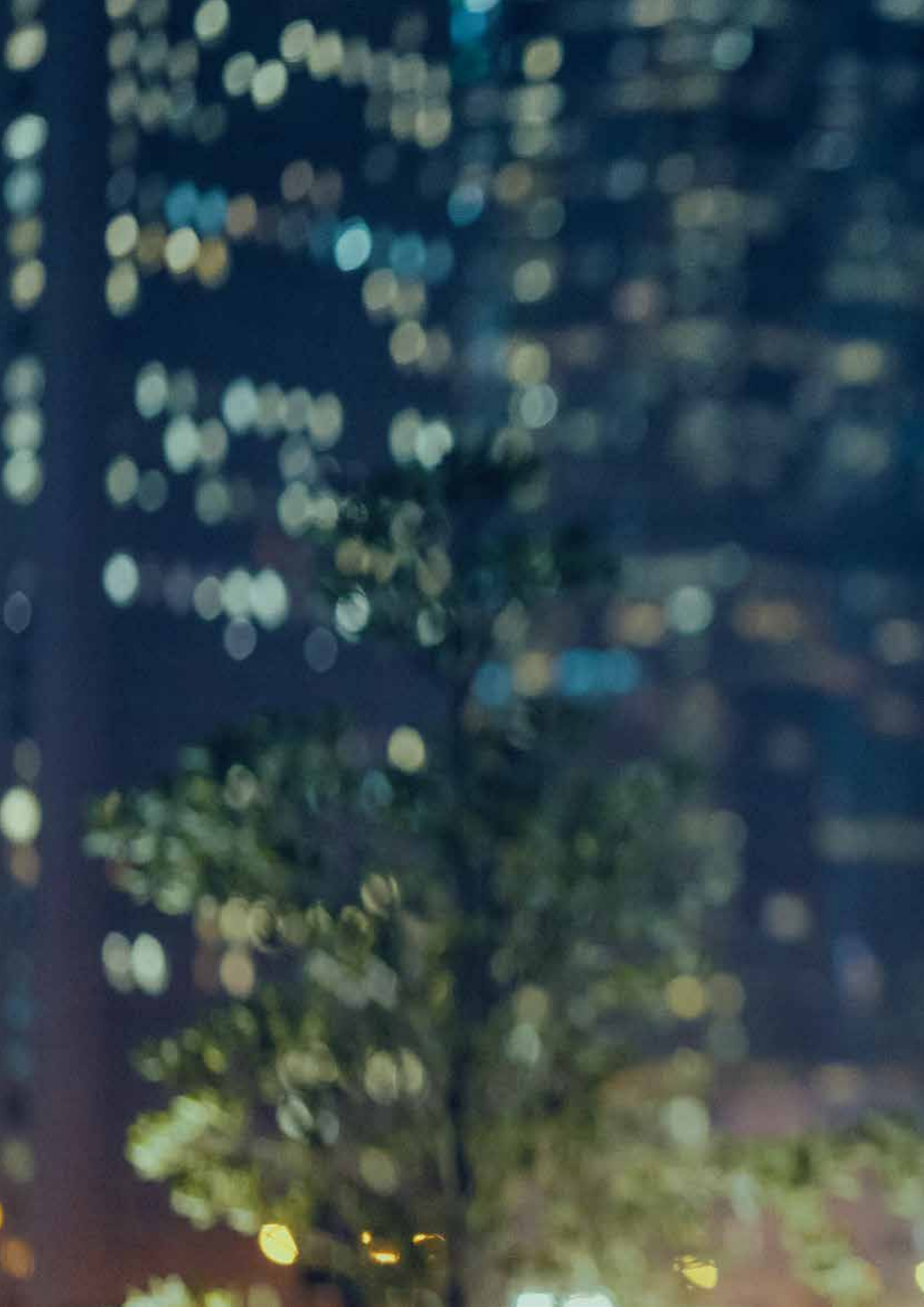
Many of GDPR's required changes come with distinct business benefits. They should mitigate the damage caused by a data breach and give institutions greater oversight of and control over the personal data in their possession. For example, the investment required to demonstrate compliance can enable more effective data management and provide clarity on the data held within an organization. This can help institutions to identify how to get the best value from customer data, including improving services.

Notification and consent requirements will increase transparency and trust for individuals, as well as more clearly define an organization's responsibility and the purpose for which it needs to collect and use data. This should help to stop institutions from collecting excessive amounts of data by limiting collection to only what they need.

Data protection and privacy is not just a compliance issue. It is also the right thing to do. Organizations that embrace current data protection reforms and privacy expectations, and successfully navigate the current changing legal and risk landscape, are finding increased business value. This is happening as their customers and employees are placing greater trust and goodwill in them, which will be invaluable in the long term. Many organizations who embraced these changes earlier, rather than later, are also gaining a competitive advantage in the market.

Financial services organizations face a special reputational risk. A **recent survey** of IT and risk or fraud decision-makers, commissioned by Varonis Systems Inc., named banking as the sector that regulators are most likely to make an example of when it comes to punishing for noncompliance. The challenge for financial services firms will be to avoid implementing the regulations too narrowly.

How financial institutions champion their customers' right to privacy and manage data securely is fast becoming a market differentiator. Rather than seeing it as a compliance issue, organizations should consider that the GDPR creates a value-added overlay that many customers are already demanding.



Contact us:

Jeremy Pizzala
EY Asia-Pacific Cyber Security Lead
jeremy.pizzala@hk.ey.com
+852 2846 9085

Nicola Hermansson
EY Asia-Pacific Privacy Lead
nicola.hermansson@nz.ey.com
+64 9 348 8148

Sean Gunasekera
EY ASEAN Cyber Security Lead
sean.gunasekera@sg.ey.com
+65 6718 1162

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

APAC no. 02033-185GBL

BMC Agency
GA 1007157

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com