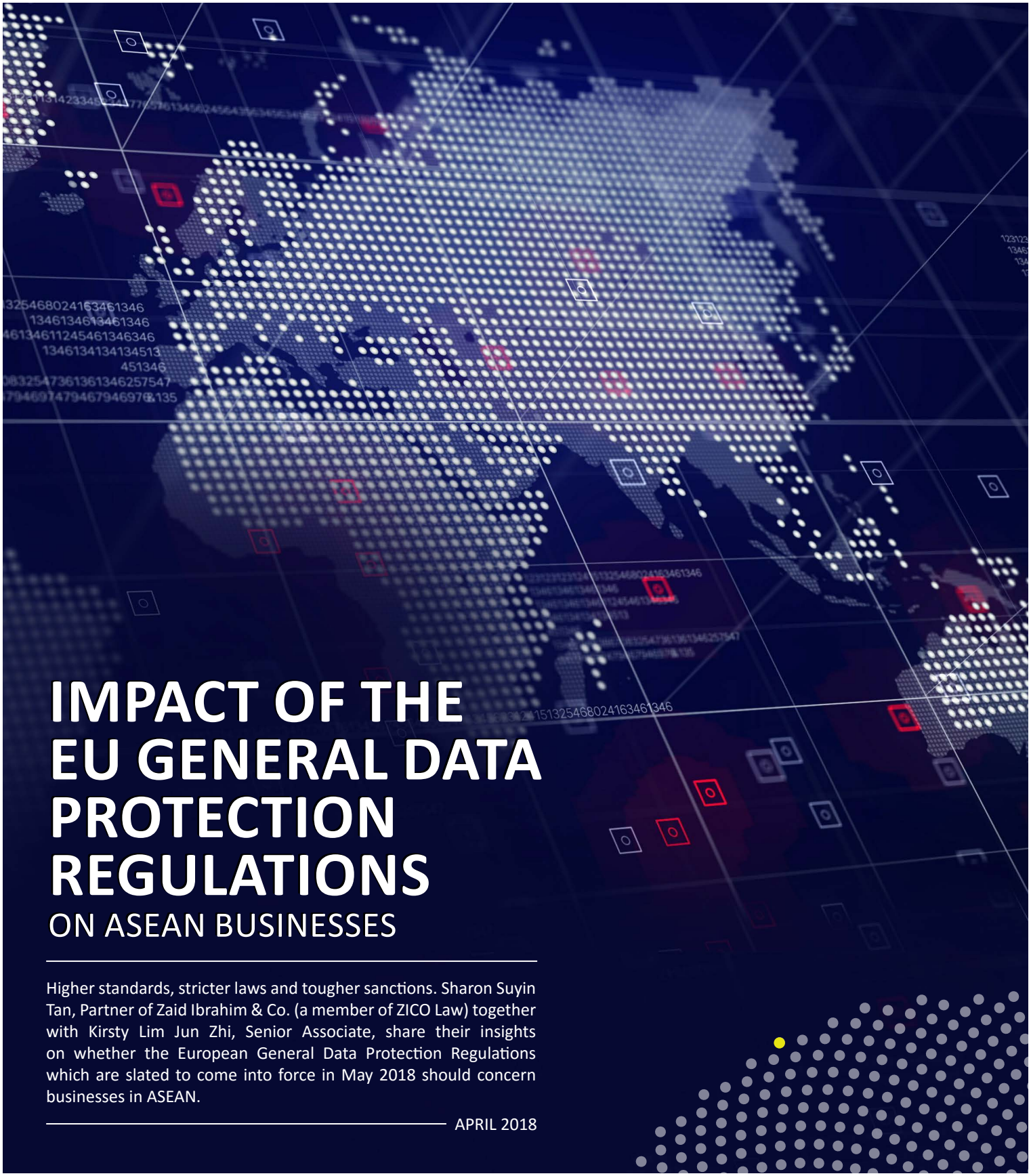
ZICO | law

ASEAN INSIDERS
by origin and passion



IMPACT OF THE EU GENERAL DATA PROTECTION REGULATIONS

ON ASEAN BUSINESSES

Higher standards, stricter laws and tougher sanctions. Sharon Suyin Tan, Partner of Zaid Ibrahim & Co. (a member of ZICO Law) together with Kirsty Lim Jun Zhi, Senior Associate, share their insights on whether the European General Data Protection Regulations which are slated to come into force in May 2018 should concern businesses in ASEAN.

APRIL 2018

BRUNEI | CAMBODIA | INDONESIA | LAOS | MALAYSIA | MYANMAR | PHILIPPINES | SINGAPORE | THAILAND | VIETNAM

Higher standards, stricter laws and tougher sanctions. ASEAN businesses have had a lot to reckon with over the past decade. On top of business challenges and having to compete with foreign entrants, they have to contend with an ever-growing list of legal and regulatory compliance obligations and local regulators playing catch-up with global trends on data flows and threats to data security. Now that the European Union has legislated to increase compliance obligations on data protection, should this concern business in ASEAN? We certainly cannot ignore it, but the question is how it will bite outside EU and what a proportionate and reasonable approach would be.

WHAT'S THE GDPR?

The EU General Data Protection Regulations will replace the EU Data Protection Directive which governs the processing of "personal data" (*i.e.* any information relating to an identified or identifiable natural person), and will apply directly in all EU member states with effect from May 2018. It is a harmonized personal data protection regime for all EU member states and is intended to provide effective protection of personal data in light of the challenges of current and anticipated technological advancements.

WE'RE BASED IN ASEAN – WHY SHOULD WE CARE?

The GDPR has extra-territorial effect, which means that it applies to individuals and organizations established **outside the EU** where it processes personal data of data subjects (*i.e.* identifiable natural persons) who are in the EU and the processing activities are related to:

(i) the offering of goods or services to data subjects; or
(ii) the monitoring of data subjects' behavior as far as their behavior takes place within the EU.

> ***"The GDPR has extra-territorial effect, which means that it would apply to individuals and organisations established outside the EU…"***

The GDPR would apply where the processing is carried out by a "controller" (*i.e.* a person which determines the purposes and means of processing the personal data, known in some jurisdictions as "data users") or a "processor" (*i.e.* a person which processes personal data on behalf of a controller). Therefore, the GDPR will apply if your business:

- serves or targets customers who are individuals residing in the EU (*e.g.* online businesses selling to customers in the EU using EU language or currency);
- processes personal data of EU individuals as part of the services you provide to your customer (*e.g.* data centers or data mining companies); or
- monitors EU individuals as part of your business, even though your operations are limited to ASEAN or Asia.

Businesses engaged in the above activities will clearly have to comply. But the issue for companies which only have a small or incidental portion of its business which fall within the purview of the GDPR is whether to plunge in and import on themselves the onerous compliance obligations, or to make a conscious decision to ring-fence compliance to those specific data sets or avoid collecting and processing such data, at least until it is clear how extra-territorial enforcement will be effected.

WHAT ARE THE PENALTIES?

While most sanctions are fixed sums, the GDPR introduces revenue based fines taking inspiration from competition law. Under the GDPR, the highest fines are **up to EUR20million** or in the case of an undertaking, **up to 4% of total worldwide turnover of the preceding year**, whichever is the higher. Fines which are imposed by reference to the revenues of an "undertaking" are generally taken to mean group companies. As such, this means that group revenues (and not only the revenue of the individual infringing company) will be taken into account in calculating fines. In addition, supervisory authorities have wide powers to issue warnings and warnings against controllers, including orders to temporarily or definitively ban processing of personal data which will definitely have wide reaching consequences on businesses.

> *The highest fines are up to EUR20million or in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year…*

Undertakings benefit from early compliance with the GDPR as the supervisory authorities administering the GDPR can take into account relevant *previous* infringements by a controller when deciding to impose administrative fines. Thus, if an undertaking has no presence in the EU which makes enforcement on it fraught with difficulty, but subsequently establishes a presence in the EU upon which proceedings can be commenced and penalties enforced, they can be haunted by their past sins. The GDPR attempts to create a nexus by introducing the obligation to appoint a Data Protection Officer within the EU jurisdiction.

WHAT IS IN THE GDPR?

The GDPR broadly maintains the data processing principles and objectives previously present in the EU Data Protection Directive, including: requirements to obtain consent, notify data subjects regarding the processing of personal data, rights of data subject to request access and correction and higher standards for the processing of special categories (or sensitive) personal data.

SO, WHAT'S NEW?

Depending on which ASEAN jurisdiction you hail from, either: a lot, or a whole lot. These data processing principles and regulations will be familiar to businesses operating in ASEAN jurisdictions with existing general data protection laws based broadly on the EU Data Protection Directive – these are Malaysia, Singapore and the Philippines. However, the GDPR has also introduced a number of new concepts which are designed to increase protection and future proof data protection regulations. Even if you already have local data protection compliance, these will be new obligations and points to consider.

Some of the key changes are:

1 | Consent is now harder to obtain.

The GDPR requires a higher standard consent for the processing of regular, non-sensitive personal data. "Consent" of the data subject must be: *"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*. As such, where businesses currently rely on implied consent for processing regular, non-sensitive personal data, this is unlikely to be permissible under the GDPR. Further, the need to have an "unambiguous indication" or a "clear affirmative act" by the data subject will render many common methods used by businesses to obtain consent as insufficient under the GDPR, these include:

- Pre-ticked boxes
- Opt-out boxes to prevent agreement/consent
- Including consent as part of general terms and conditions
- Silence or inactivity of the data subject

Further, multi-purpose catch-all consents which are very commonly used in ASEAN are unlikely satisfy the requirement that consent must be specific and informed.

In the age of cloud computing and blockchain technology which is expected to revolutionise data processing, these raise additional considerations on cross-border data flows and personal data being on decentralized autonomous organisations. Data protection notices and consents will need to be reviewed to cater for these, too.

> *Consent is now harder to obtain – the need to have an "unambiguous indication" or a "clear affirmative act" by the data subject will render many common methods used by businesses to obtain consent as insufficient…*

2 | Higher standards for explicit consent.

If the standard for obtaining 'regular' consent has been raised to require: an "unambiguous indication" or a "clear affirmative act"; an even higher standard would need to be applied in order to obtain "explicit consent", which is one of the methods of validating the processing of sensitive personal data. The Working Party established by the European Parliament have suggested that two-step verification processes for obtaining consent may be one way to ensure that the explicit consent provided is valid *e.g.* indicating consent on a website and confirming the consent by subsequently having to click on a verification link sent to the data subject's email address.

3 | Stringent data breach notifications.

Controllers are required to notify a personal data breach to the supervisory authority without undue delay and where feasible within **72 hours** unless the data breach is unlikely to result in a risk to the individuals. Where the breach is likely to result in a high risk to individuals, the controller will have to inform the data subjects of the breach without undue delay (unless prescribed exceptions apply). Businesses would now need to develop and implement data breach response plans to enable them to effectively comply with the data breach notification requirements under the GDPR.

> *Businesses would now need to develop and implement data breach response plans to enable them to effectively comply with the data breach notification requirements under the GDPR.*

4 | New obligations on processors.

Previously, data protection obligations were only imposed directly on controllers; however the GDPR imposes new obligations directly on processors. These obligations include:

- Implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk to personal data
- Data breach notifications
- Maintaining a record of all categories of processing activities carried out of behalf of the controller
- Imposing, by way of contract, prescribed obligations on sub-processors appointed by the processor
- Designating a data protection officer and ensuring the data protection officer is involved in all issues which relate to the protection of personal data
- Complying with restrictions of transfers of personal data to third countries or international organizations

Pre-GDPR and under local data protection laws in Malaysia and Singapore, security obligations were imposed directly on controllers, who in turn imposed them contractually on processors. Under the GDPR, the processors are themselves liable for breaches of the above GDPR obligations.

5 | New right to be forgotten and data portability.

Data subjects will have the right to require the controller to erase personal data concerning him or her without undue delay. Where the controller has made the personal data public, the controller, taking into account available technology and cost of implementation, must take steps to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. In relation to the right to data portability, the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance for the controller. Businesses that process large amounts of personal data will need to take into consideration how they can effectively comply with these obligations. Many businesses collect, store and distribute personal data automatically and in a manner which would render it difficult for the business to efficiently trace, compile and erase (if necessary) the personal data it would have on a data subject. As such, businesses may need to possibly devote additional time and resources to scrutinize its current data flows to determine how it can give effect to the right to be forgotten and right to data portability.

> *Many businesses collect, store and distribute personal data automatically and in a manner which would render it difficult for the business to efficiently trace, compile and erase (if necessary) the personal data it would have on a data subject.*

YOU CAN'T CATCH ME, I'M NOT IN THE EU!

> *Any enforcement actions which the supervisory authorities are minded to take against businesses based in ASEAN which are caught by the GDPR would likely be imposed on the business' representative in the EU.*

Where the GDPR applies to the controller or processor, the GDPR requires the controller or processor to designate in writing a representative in the EU, *i.e.* a natural or legal person established in the EU who represents the controller or processor with regard to their respective obligations under the GDPR. This requirement would not apply if the controller or processor does not process: personal data on a large scale; sensitive personal data or data relating to criminal convictions, and the processing is not likely to result in a risk to the rights and freedoms of individuals. As such, any enforcement actions which the supervisory authorities are minded to take against which have no presence in the EU would likely be imposed on the business' representative in the EU.

TO DO? OR NOT TO DO?

This is a EUR20million question. For businesses in ASEAN countries which do not currently have data protection laws, the prospect of complying with the GDPR would seem to be a huge undertaking. But even for businesses in Malaysia, Singapore and the Philippines, the cost and resources which would need to be dedicated in order to ensure effective compliance with the GDPR is likely to be considerable, especially given the imminent deadline when the GDPR comes into force in May 2018. Businesses with presence or dealings across different ASEAN countries with different data protection regimes will perhaps have some difficulty in deciding how it will manage personal data across these different regimes, as rolling out personal data compliance in regimes which do not have data protection laws may be viewed by businesses as a costly endeavour. As ever, businesses would have to weigh the cost of compliance against the risks of non-compliance. But given that the risks involve fines of up to EUR20million or up to 4% of total worldwide turnover of the preceding year, this is not a decision which can be taken lightly.

But perhaps we can take heart that the EU GDPR requires some nexus with the EU in order for it to apply. The Recitals of the GDPR indicate that in order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Mere accessibility of a website, of an email address or use of language in the country where the controller is located *per se* is insufficient to establish such use. But where there are other factors which show an intention to deal with persons in the EU, such as use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, this tips the balance in favour of application of the GDPR. Thus, companies should take into account these nuances when reviewing their marketing and client communications to avoid inadvertently falling within the scope of the GDPR.

OUR ASEAN TAKE

The sea of change in data protection regulation while originating in the EU will eventually hit our ASEAN shores. On 31 January, the European Commission endorsed horizontal provisions for cross-border data flows and personal data protection in trade negotiations. As the protection of personal data is considered a fundamental right in the EU, the EC considers that these principles cannot be the subject of negotiations and if accepted by member states will be "exported" through Free Trade Agreements and Bilateral Investment Agreements between the EU and other countries. Three countries in ASEAN (Singapore, Malaysia and the Philippines) already have some form of data protection laws of general application. Those who have embarked on compliance with these laws will need to upgrade their compliance if the EU GDPR applies to them, and it's a steep learning curve. But mostly, companies with no presence in the EU seem to be taking a wait and see approach, taking tentative steps to see how the GDPR is enforced outside the EU, and prioritising their efforts to make the changes which are most obviously required and visible and examining the nexus within the EU. Mind you, the sword of Damocles awaits flagrant offenders should they later come within the reach of the GDPR.

If you have any questions or require any additional information, you may contact us or the ZICO Law partner you usually deal with.

Sharon Tan
Partner
sharon.suyin.tan@zicolaw.com
t. +603 2087 9999
t. +603 2087 9849

Sharon Tan advises on a broad spectrum of corporate and commercial matters, with industry expertise in the technology, communications and multimedia sector. Sharon also advises on regulatory compliance and operational arrangements in the sector including on outsourcing, and on corporate transactions in the industry such as acquisitions and joint ventures. Sharon also advises on electronic commerce transactions, payment systems and general corporate and commercial law, including personal data protection.

Kirsty Lim Jun Zhi
Senior Associate
kirsty.j.lim@zicolaw.com
t. +603 2087 9929

Kirsty Lim's key practice area is corporate and commercial, she frequently advises multinational companies on matters involving its businesses and investments in Malaysia, including in the areas of M&A, competition, distribution and franchise. Kirsty also advises on a range of regulatory and compliance matters including those in the communications, media, strategic trade, postal, franchise, logistics, tourism and wholesale retail trade sectors. Kirsty is also experienced in designing personal data protection compliance programmes for local companies, and has advised extensively on personal data protection and confidentiality issues.

This article was edited by ZICO Knowledge Management.

ZICO | law

ASEAN INSIDERS,
by origin and passion

30 Years of Growth & Innovation 1987-2017

BRUNEI | CAMBODIA | INDONESIA | LAOS | MALAYSIA
MYANMAR | PHILIPPINES | SINGAPORE | THAILAND | VIETNAM