ASEAN PATH

DO YOU PROCESS PERSONAL DATA FROM EU INDIVIDUALS?

WELCOME

The European Union (EU) is setting a new global standard for personal data privacy which is widely expected to exert a profound effect on data policies worldwide. Taking effect on 25 May 2018, the EU General Data Protection Regulation (GDPR) seeks to extend the reach of EU data protection law, and it is set to impact businesses far beyond the borders of the EU.

Regardless of whether your company has a presence in the EU, it may still fall within the jurisdiction of the GDPR if it is in any way involved in the processing of personal data of individuals within the European Union. Those affected companies must now comply with the GDPR's numerous requirements, such as the necessity of having a legal basis for processing data, or obligations to notify any data breach to affected individuals and authorities, to name a few. Needless to say, the possibility of fines of up to 4% of annual global revenue, or EUR 20 million, are certain to provide companies with a sobering incentive to adhere to the new Regulation. It is therefore of paramount importance that Asia-based companies get to grips with the impact of the GDPR and formulate clear strategies to ensure compliance with its far-reaching provisions.

The first section of this issue of ASEAN Path will provide you with the necessary guidance to determine whether your business will fall under the GDPR's scope. We then provide an overview and analysis of the several obligations arising under this new regulation. The third section lays out the various financial and non-financial penalties that may apply in instances of non-compliance. Finally, a brief list is provided at the end of this issue outlining certain appropriate measures to consider implementing, in order to ensure full compliance with the terms of the new GDPR.

We hope that this edition of ASEAN Path will provide you with some useful guidance on this important topic. As always, we welcome the opportunity to discuss in depth your concerns regarding the impact of the GDPR on your business, in any of the countries where DFDL or its associated firms operate.

Audray Souche
Partner; Country Managing Director, Thailand
P: +66 26 363 282
E: audray.souche@dfdl.com

ASEAN PATH is a series of white papers prepared by DFDL's experts aiming to assess, in more depth, compelling issues arising from the regional economic integration under the auspices of the Association of Southeast Asian Nations ("ASEAN") Economic Community Blueprint. The articles are based on an in-depth legal analysis of the local and ASEAN legal framework from the perspective of a practitioner assisting foreign and ASEAN investors in their investments and operations throughout various ASEAN Member States. All articles are accessible on our website: www.dfdl.com.

INTRODUCTION

Less than 20 years ago, three quarters of all stored information was in non-digital form: names were itemized on municipal registers, identification numbers were held in national healthcare systems, and passport numbers were recorded on immigration forms. Today, more than 98% of the world's stored information is in digitized form: our collective 'data' now primarily resides on a dematerialized, open-ended, global digital cloud. In this era of unprecedented online connectivity comprising email addresses, purchase preferences, reading frequencies, travel plans, and many more, all of this personal information is now within reach to be processed for a multitude of analytical purposes. In light of numerous recent privacy related scandals, the safety and security of our data has rapidly come to the fore of heightened attention and debate. New regulations have emerged in a number of countries to enshrine data protection principles. The European Union ("**EU**") has been at the vanguard in introducing a new phase of the regulatory process with the impending entry into force of European regulation 2016/679. This *General Data Protection Regulation* ("**GDPR**" or the "**Regulation**")[1] is squarely aimed at the protection of individuals with regard to the processing, securing, and free movement of their personal data.

Due to enter into effect on 25 May 2018, the GDPR will replace the Data Protection Directive 95/46/EC that was adopted in 1995. This wide-ranging reform is geared towards extending and enhancing individual data protection within the EU from privacy and data breaches. It will greatly expand data privacy rights and means of legal recourse and harmonize data protection legislation throughout the continent.

This new regulation is likely to exert significant influence on a host of businesses operating around the globe - not merely EU-based companies. It is thus crucial for companies established in Asia to fully understand the scope of the GDPR, be cognizant of its underlying obligations, and aware of the associated sanctions and penalties. Upon assessing the applicability of the GDPR to their operations, businesses must pursue proper planning of appropriate measures to ensure compliance with its provisions.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

WHO IS AFFECTED BY THE **GDPR**?

The GDPR regulates the manner in which businesses process and manage personal data. To ascertain whether your own business will fall within the purview of this Regulation's provisions, you must now consider whether you conduct any data processing activities within the European Union. If it transpires that the GDPR does apply, you will have to take action to determine the exact role and nature of your business as a data controller or processor.

WHICH ACTIVITIES ARE SPECIFICALLY SUBJECT TO THE **GDPR**?

The GPDR applies to the *processing of personal data*,[2] i.e. the processing of any information related to an identified or identifiable individual (as opposed to a legal entity), also known as a *data subject* under the GDPR. This definition encompasses the collection, recording, use or deletion of names, physical or e-mail addresses, phone numbers, locations, banking information, health information, and many more. On this basis, any access of a database containing personal data, sending promotions or newsletters via email, or even simply posting someone's personal information on social media, will clearly fall within the parameters of the GDPR.

Therefore, *any* type of business that processes the personal data of *data subjects* may be subject to the GDPR. Physically storing collected data for the purposes of targeted advertising or shipping of goods are equally as exposed as more conventional e-commerce businesses that gather significant amounts of personal data as a matter of course.

It is worth bearing in mind that the definition of *data subjects* encompasses not only an enterprise's customers or clients, but also its own employees. Furthermore, the Regulation may also extend to other legal entities that regularly process large amounts of data, such as public authorities or governmental departments.

[2] Article 2 of the GDPR

WHERE DOES THE **GDPR** APPLY?

The biggest change to the EU data privacy regulatory environment heralded by the new Regulation lies in the expanded territorial scope of its application. Now, any business that processes *personal data* on EU territory, regardless of the legal entity's location, must abide by the new Regulation.

The GDPR thus applies not only to EU companies (including EU companies doing business in Asia through local subsidiaries or branches) but also to any Asia-based companies (as elsewhere in the world) operating in Europe. For instance, a local startup based in Thailand developing a new app for a global audience will potentially be subject to the GDPR's provisions.

The widening of this Regulation's jurisdiction beyond the EU, also known as *extra-territorial applicability*, is particularly broad: Asia-based companies may fall under the GDPR's scope in the following three different scenarios.[3]

[3] Article 3 of the GDPR

Where the business has an establishment in the EU

Firstly, the GDPR applies to any entity which has an *establishment* in the EU, and where personal data is processed in the normal course of such an establishment's activities, regardless of where the processing takes place.

Establishment is defined as the "*effective and real exercise of activity through stable arrangements,*" [4] implying the stable presence of personnel and technical resources within the EU, although the legal form of such arrangements is not a determining factor.

Thus, if your business is based in Asia but has an *establishment* in the EU involved in the processing of personal data, such as a single representative or sales outlet, it would fall within the jurisdiction of the GDPR.

Where the business offers goods or services in the EU

Secondly, any non-EU established business that processes the personal data of individuals within the EU for the purposes of *offering of goods or services* to such individuals, e.g. through a website, will be subject to the GDPR. This qualification is not subject to the actual performance of a payment transaction by the individual.

Whether a company is actually offering goods or services to individuals in the EU will be determined on a case-by-case basis, with due consideration paid to the *intent* of the company to do so. It appears that the mere accessibility of a website by an EU audience is not sufficient to demonstrate such an intention, neither is the use of a European language also commonly used in the company's own country. However, using an EU language or currency and the ability to order goods and services in that other language, mentioning EU clients on a website, using an EU top-level domain name, or targeting EU consumers through advertising, are factors that may demonstrate a non-EU business's intention to offer goods or services to EU data subjects.[5]

Where the business monitors the behaviour of individuals in the EU

Thirdly, a business which has no establishment in the EU nor offers goods or services to EU data subjects may still be subject to the GDPR if it processes individual personal data for the purposes of *monitoring their behaviour* within the EU.

Similar to the offering of goods and services, what constitutes monitoring will be determined on a case-by-case basis. This clearly implies the tracking of individuals over the internet for commercial purposes in order to profile them and to analyze and predict their preferences, behaviours, and attitudes.[6]

Therefore, if your company's website or app uses cookies and other tracking methods to monitor the behaviour of individuals within the EU, this would fall within the remit of the GDPR.

The GDPR applies its protections to all *data subjects*, regardless of their nationality or residence,[7] as long as they are '*in*' the EU. *Data subjects* therefore, need not necessarily be EU citizens or residents. If your

[4] Recital 22 of the GDPR
[5] Recital 23 of the GDPR
[6] Recital 24 of the GDPR
[7] Recital 14 of the GDPR

business collects personal data on Asian citizens while they are on vacation in the EU for example, such data processing may still be subject to the GDPR.

Data processors vs. data controllers

The Regulation distinguishes between *data controllers* and *data processors*, with different obligations applying to both categories. A *controller* determines 'why' and 'how' personal data should be processed, whereas a *processor* is responsible for processing the personal data on behalf of the controller (such as a cloud service provider).

Under the GDPR, processors have specific legal obligations and legal liability in respect of a data breach. However, this does not mean that controllers are released from any liability when data processors are involved. The controller must ensure that the data processor offers sufficient guarantees regarding the GDPR requirements, and these guarantees must be clearly stated in a written contract entered into between them.

It is therefore imperative to determine your company's role as a data controller or data processor, in order to comprehensively grasp the specific obligations and requirements of the GDPR that will apply to your company.

Considering the extra-territorial applicability of the GDPR, if your own business falls under either scenario, whether as a data controller or processor, it is crucial that measures be implemented to ensure that the business is in line with the GDPR's obligations as of May 25th.

What are the obligations under the **GPDR**?

A company is required to comply with several conditions in order to lawfully process personal data pursuant to the GDPR provisions. The processing should be *lawful and transparent*, for a *specified purpose*, *limited to the relevant data necessary* in relation to this purpose, and *appropriately secured*.[8] At a glance, businesses must have a valid legal basis in order to process personal data, must adequately uphold the rights of data subjects, along with being responsible for and clearly demonstrating compliance with GDPR principles.

Particularly noteworthy is that specific provisions apply to certain categories of 'sensitive' persona data, such as political opinions, racial or ethnic origin, or those relating to criminal convictions and offences.[9]

Having a lawful basis for processing activities

According to the GDPR, processing personal data is only permissible if there is a lawful basis to do so as listed under its provisions. [10] All businesses must then identify the most appropriate grounds, clearly document their choice, and directly inform individuals about the lawful basis for processing their personal data. Such processing must be based on one of the following grounds:

- **Consent**: the individual has expressly consented to the processing of their personal data for a specific purpose;
- **Contract**: the data processing is necessary to fulfill an obligation arising from a contract with the individual;
- **Legal obligation**: the data processing is necessary to comply with a legal obligation;
- **Vital interests**: the data processing is necessary to protect an individual's vital interests;
- **Public task**: the data processing is necessary to perform a task in the public interest; and
- **Legitimate interests**: the data processing is necessary for legitimate business interests, but only to the extent that the individual's rights are not seriously impacted or overridden by such business interests.

The appropriate legal basis for your business will hinge upon the specific purposes and context for processing personal data. In most cases, companies are likely to have a choice in electing between consent or legitimate interests as the basis for processing their customers' personal data. Concerning the employees of a business, data processing may be necessary to fulfill certain obligations stipulated in their employment contracts for instance.

On the issue of a data subject's consent, the GPDR lays down stringent rules. The request for consent should be distinct from other terms and conditions, and should employ "*clear and plain language,*" [11] and provide the data subjects with sufficient information regarding the processing of their data. Such consent must therefore be *free*, *specific* (i.e. only provided for the purposes explicitly stated in the request), *informed and unambiguous*. It must also result from an *affirmative act*, implying a positive opt-in by

[8] Article 5 of the GDPR
[9] Articles 9 and 10 of the GDPR
[10] Article 6 of the GDPR
[11] Paragraph (11) of Article 4 of the GDPR

checking a box online or signing a form, and not inferred from silence or pre-ticked boxes. Furthermore, the opportunity to easily withdraw consent must be granted to all data subjects. Additional specific conditions also apply to child's consent.[12] In conclusion, obtaining consent that satisfies the GDPR's standards may be laborious - it would be wise to look for a different legal basis for data processing where possible.

In any event, the legal basis applicable to your business must be determined before beginning to process personal data. This will necessitate a thorough assessment, as it may become more complex and cumbersome to subsequently switch from one set of legal grounds to another.

Ensuring data subject's rights

Under the GDPR, *data subjects* are given wide-ranging rights to have control over their personal data. The numerous obligations incumbent on businesses processing such data are geared towards the protection of EU individual rights including, among others:

- **Information and transparency**: individuals have the right to be informed about the collection and use of their personal data. *Data subjects* must be provided with a minimum level of information at the time that their personal data is obtained, including but not limited to the identity and contact details of your company, the purposes of the processing, the legal basis for doing so, retention periods for the data to be stored, and how consent may be withdrawn.[13]
- **Data accessibility and portability**: upon request by any *data subject*, confirmation must be provided as to whether their personal data is being processed by the relevant company. If this is the case, he or she must be duly notified about the processing and provided with a free electronic copy of the personal data that is being processed. Additionally, *data subjects* have the right to demand that their personal data be returned or transmitted to another company in a commonly use and machine-readable format.[14]
- **Data clearing**: also known as the *right to be forgotten*, it entitles the data subject to request that their personal data be erased, if the data is no longer relevant to the processing purpose and/or the data subject withdraws its consent. Nonetheless, a small number of scenarios remain where a business may refuse to comply with such a request.[15]
- **Automated decision making and profiling**: in some circumstances, individuals have the right not to be subject to a decision that is based solely on automated processing, e.g. an online decision to award a loan, and can request human intervention and contest the automated decision.[16]

In addition, if a company receives a request from a *data subject* that wants to exercise his or her rights, the company must respond without undue delay, i.e. within one month of receiving the request in most cases.[17]

Accountability for compliance with the GDPR

Pursuant to the accountability principle of the GDPR, all businesses are *responsible for, and must be able to demonstrate, compliance* with the other principles of the Regulation.[18] This means that companies have

[12] Article 8 of the GDPR
[13] Articles 12 and 13 of the GDPR
[14] Articles 15 and 20 of the GDPR
[15] Article 17 of the GDPR
[16] Article 22 of the GDPR
[17] Article 12 of the GDPR
[18] Article 5 of the GDPR

to be proactive and systematic in their approach to data protection and must be able to supply evidence of the steps they take to satisfy their obligations and protect individuals' rights.

While there is no exhaustive list of measures to be put in place to comply with this principle, the GDPR provisions state that a company has a duty to implement *technical and organizational measures* which are to be *risk-based* and *proportionate*, and *updated as necessary*.[19] However, some risk-based measures are specifically required by the Regulation, including the following:

- **Data protection by design and by default**: the GDPR calls for businesses to implement appropriate technical and organizational measures to protect the rights of data subjects by including data protection mechanisms at the early stages of designing new systems to process personal data, using *pseudonymization* for instance, but also by having the most privacy friendly setting as the default setting.[20]
- **Record processing activities**: Most businesses are required to maintain a record of their processing activities, containing information on the purposes of the processing, data sharing, retention, consent where relevant, and personal data breaches if applicable.
- **Notification of breach**: If a *data breach* occurs, i.e. personal data is disclosed to unauthorized recipients or altered and is likely to result in a risk to an individual' rights and freedoms, the relevant authority must be notified within 72 hours of becoming aware of such a breach. In certain circumstances, an enterprise may also be required to inform all individuals affected by a data breach.[21]
- **Data Protection Officer (DPO)**: in addition to internal record keeping requirements, an enterprise may be required to appoint a DPO, if the core business activities involve regularly and systematically monitoring data subjects or processing special categories of data on a large scale (i.e. sensitive data).[22] This DPO, who may be a staff member or an external service provider, must comprehensively monitor compliance.

There are several other measures that may be pursued with regard to the accountability principle, such as adopting and implementing data protection policies, adhering to relevant codes of conduct, signing certification schemes or even carrying out data protection impact assessments (DPIA). It is essential to understand that accountability is an opportunity to conspicuously demonstrate and affirm that your business respects individual privacy, and therefore cultivate and maintain the trust of customers or clients.

Non-EU businesses subject to the application of the GDPR will need to appoint a representative in the EU – any private company offering such services - as a point of contact for EU data subjects and data protection authorities.[23] This representative may face enforcement actions in the event of your company's failure to comply with the GDPR. It is thus unlikely that it would represent you without strong contractual indemnities first being in place.

Given the nature and extent of the obligations provided for under the GDPR, any business in Asia coming under its scope needs to pay close attention to these compliance obligations, particularly since any failure to do so could result in heavy fines.

[19] Article 23 of the GDPR
[20] Article 25 of the GDPR
[21] Articles 33 and 34 of the GDPR
[22] Article 37 of the GDPR
[23] Article 27 of the GDPR

WHAT SANCTIONS MAY APPLY?

The risks associated with failing to comply with the GDPR are steep: it can expose businesses to substantial penalties, ranging from corrective measures to administrative fines.

There is a tiered approach to fines. On the lower end, companies can be fined up to EUR 10 million or 2% of their annual global revenue, whichever is higher, for infringements related to data protection by design and by default, records of the processing activities, and security of processing for instance. On the upper level, companies that are in breach may be fined by up to 4% of their annual global turnover or EUR 20 million, whichever is greater, for the most serious infringements, namely those related to the issue of consent and data subjects' rights.[24]

A range of corrective measures may also be imposed, such as ordering a temporary or permanent ban on processing, a restriction on erasing data, or suspending data transfers to third countries.[25] Furthermore, one must consider the reputational damage and loss of consumer trust along with compensation claims for damages suffered that may result from a single breach.

In any event, the costs of falling foul of the GDPR are much more onerous than any investment made to abide by it. If your Asian business falls within its scope, it is recommended to immediately map out your current data processing activities and begin preparing for the imminent enforcement of the GDPR.

[24] Article 83 of the GDPR
[25] Article 58 of the GDPR

HOW TO ENSURE COMPLIANCE?

In order to prepare suitable measures to ensure compliance with the GDPR, businesses must at the very least take the following steps to re-evaluate their internal processes:

- Ensure that key in-house people are aware of the coming shift,
- Identify the relevant legal basis for data processing,
- Document and record the current processing of personal data,
- Assess the IT, organizational, and data protection measures in place,
- Review the current procedures regarding data subjects' rights,
- Address the potential need to appoint a Data Protection Officer.

Some provisions of the Regulation will have more effect on some businesses than others, depending on their role, or the quantity of data being processed for instance. It is therefore crucial for every company to properly assess the impact of the GDPR and understand the resulting obligations in order to set sufficient safeguards and specific measures into place.

CONCLUSION

Unlike the EU, Asia does not yet have a harmonized approach towards data privacy, and local legislation is far from comprehensive in many jurisdictions.

In the Philippines for instance, strong data protection policies have already been implemented with the 2012 Data Privacy Act ("**DPA**"). Through proper compliance with the DPA's high standards, Filipino businesses will already meet many of the GDPR requirements, and this will serve as a solid starting point to build from. However, new obligations under the Regulation need to be carefully addressed, making it critical that all companies subject to the GDPR in the Philippines also prepare for its entry into force. At the other end of the spectrum, there are many Asian countries where data protection rules are very limited, and occasionally non-existent. In Thailand for instance, the lack of regulation has led to unfortunate incidents of misuse of consumer data, and the fast-growing development of online and mobile banking and E-commerce calls for swift action in the country. In light of the looming passage into law of the GDPR, and the ripple effects it will have on Thailand's digital economy, the Ministry of Digital Economy and Society has prepared a new draft legislation to comprehensively address data privacy issues. It is expected to be finalized by the end of the year for Cabinet approval prior to enactment. In nations where no data protection rules exist, such as Cambodia, the learning curve will be even more challenging.

The GDPR should serve as a wakeup call for all local governments to put data privacy at the forefront of their legislative efforts, especially in light of the exponential and pervasive rise of E-commerce and fintech services. This European Regulation is likely to serve as a model for best practices regarding data privacy around the world and in Asia.

In summary, while your business may not yet be subject to the GDPR rules today, their entry into force is approaching, with numerous nations fast at work on drafting similar legislation in response to the growing demands for greater consumer data protection. This is especially pointed in light of a multiplicity of privacy related scandals (such as the Facebook-Cambridge Analytica Scandal) around the world that have mobilized citizens to pressure their government leaders to take matters of individual privacy seriously. Complying with the GDPR data standards will resolutely demonstrate your company's desire to protect customers' interests. On the contrary, by falling short of the heightened expectations that consumers now place on companies dealing with their personal data, you run the risk of forever losing your consumers' trust, which in the current global context of people concerned by data privacy, could be detrimental to your business.

CONTRIBUTORS

Marion Lagrange
Consultant
Marion.Lagrange@dfdl.com

Maly Courtaigne
Managing Director (Singapore)
Maly.Courtaigne@dfdl.com

Audray Souche
Partner, Managing Director (Thailand)
Audray.Souche@dfdl.com

DFDL offices

Bangladesh
Dhaka
bangladesh@dfdl.com

Cambodia
Phnom Penh
cambodia@dfdl.com

Myanmar
Naypyidaw
Yangon
myanmar@dfdl.com

Lao PDR
Vientiane
laos@dfdl.com

Singapore
Singapore
singapore@dfdl.com

Thailand
Bangkok
Samui
thailand@dfdl.com

Phuket
phuket@dfdl.com

Vietnam
Hanoi
hanoi@dfdl.com

Ho Chi Minh City
hcmc@dfdl.com

***DFDL collaborating firms**

Cambodia*
Sarin & Associates, Phnom Penh
cambodia@dfdl.com

Indonesia*
Mataram Partners, Jakarta
indonesia@dfdl.com

Philippines*
Ocampo & Suralvo Law Offices, Manila
info@ocamposuralvo.com