EUROPEAN GDPR 2 YEARS ON:

What lessons can be drawn from the European Experience for the Southeast Asian Region?

June 2020

INTRODUCTION

Two years ago, the most visible and tangible impact of the entry into force of the General Data Protection Regulation ("**GDPR**" or "**Regulation**")[1] for individuals all around the globe was an unprecedented wave of emails from businesses changing their privacy policies and seeking consent to store and process data. Primarily aimed at protecting fundamental rights and freedoms of individuals with regard to their personal data, this regulatory framework is also geared towards allowing the free flow of personal data and the development of the digital economy across the European Union ("**EU**"). Two years later, on 25 May 2020, being the second anniversary of the GDPR's entry into force, the time has come to assess the achievements of the Regulation and draw useful lessons for other regional blocs moving towards similar data protection regimes such as in Southeast Asia, albeit not in a centralized manner like the EU.

According to Article 97 of the Regulation, the European Commission was supposed to submit a first report on the evaluation and review of the GDPR by 25 May 2020. Although publication of that report has been postponed indefinitely, some relevant European bodies such as the Council of the EU and the European Data Protection Board ("**EDPB**")[2] have already contributed to this evaluation by publishing their findings and positions on the implementation of the GDPR.[3] Furthermore, relevant stakeholders such as the EU Member States and the supervisory authorities were also provided with the opportunity to share their respective experiences and input for the purpose of this evaluation.

The wide-ranging reforms heralded by the Regulation have unquestionably forced organizations to give much more consideration to the data they process, resulting in a heightened level of awareness surrounding data protection issues. With most businesses developing a compliance culture and citizens becoming more conscious of their rights, convergence towards high data protection standards is progressing at an international level. Over the course of the last two years, the European Court of Justice ("**ECJ**") and the EDPB have provided useful clarification and guidance on a number of topics such as consent procurement, data handling processes and the regulation of website cookies. Nonetheless, all stakeholders have been continuing their rallying cry calling for greater interpretational clarity and consistency across the EU in the application of certain requirements.

[1] Regulation ("**EU**") 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[2] The European Data Protection Board ("**EDPB**") is an independent European decision-making body established by the GDPR, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.

[3] Note no. 13599/19 of the Council of the European Union regarding the Preparation of the Council position and findings on the application of the GDPR and Contribution of the EDPB to the evaluation of the GDPR under Article 97, adopted on 18 February 2020.

A POSITIVE VIEW: INCREASED AWARENESS ON PERSONAL DATA PROTECTION ISSUES

Given the GDPR's wide scope of applicability and the nature and extent of its underlying obligations, businesses have had to be particularly cautious and mindful about their data processing activities. This includes the collection, use, sharing, security and storage of personal data within the company as well as with business partners and service providers. The GDPR's launch has resulted in growing awareness of data protection issues at all levels and the considerable costs of failing to comply with its provisions. These range from substantial fines to reputational damage and loss of consumer trust, all of which have undoubtedly concentrated the minds of many on these concerns.

Pursuant to the accountability principle,[4] businesses have to be proactive and systematic in their approach to data protection and able to supply evidence of the steps taken to satisfy GDPR requirements and protect individual rights. In adherence to the data minimization and data protection by design principles,[5] businesses have begun to review and reassess the relevance and need for processing personal data to ensure that it is limited to the expressly necessary purpose.

As an illustration, the number of data breach notifications[6] from businesses to personal data supervisory authorities has increased by 12.6% between the period 25 May 2018 to January 2020. In 2019, businesses on average reported 278 personal data breaches per day.[7]

The GDPR and its wide publication have served as a catalyst for the worldwide emergence of data protection laws with more and more countries beginning to adopt more stringent legal frameworks with strict and consistent data protection provisions at their core. To name a few:

- Thailand enacted the Personal Data Protection Act[8] in May 2019 and similarly incorporates a number of the GDPR's main principles.
- The Lao PDR's Law on Electronic Data Protection, enacted in 2017, came into force shortly after the GDPR in August 2018.[9]
- Brazil passed its own General Data Protection Law[10] in 2018 which openly references the GDPR.

Despite the efforts being undertaken at a Southeast Asian level, the EU's "Adequacy Decisions" (a list of countries considered by the EU to have an "adequate" level of data protection), to date, does not contain any Southeast Asian country[11] despite several Southeast Asian nations (including Singapore, Malaysia, Taiwan and the Philippines) putting into place personal data protection frameworks long before the GDPR.

While it is true that the GDPR was not the first consolidated data privacy legislation, the wide ranging applicability and collective harmonization by all EU Member States served as a wakeup call for governments across the world to place data privacy at the forefront of their legislative efforts. Other nations are now considering their own dedicated data protection regulatory approaches such as India, where a Personal Data Protection Bill is currently making its way through the Indian parliament. The introduction and effectiveness of the GDPR can thus be rightly recognized as a watershed moment for personal data protection worldwide and the consequent convergence of local rules is opening up new opportunities for safe data flows across the world.

[4] In accordance with Article 5 of the GDPR, all businesses are responsible for, and must be able to demonstrate, compliance with the principles relating to processing of personal data under the GDPR.
[5] Under the GDPR, data processing should be limited to the relevant data necessary in relation to a specified purpose. Further, 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.
[6] 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.
[7] DLA Piper GDPR data breach survey: January 2020
[8] Personal Data Protection Act B.E. 2562 (2019)
[9] Law on Electronic Data Protection (No. 25/NA, 12 May 2017)
[10] Law No. 13709 of August 14, 2018, 'Lei Geral de Proteção de Dados' or LGPD
[11] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

FURTHER GUIDANCE PROVIDED BY EU BODIES' DECISIONS AND THE ECJ

Consent related issues

In October 2019, the ECJ issued a ruling on consent for the use of cookies and other tracking technologies in the Planet49 case.[12] In the eyes of the Court, pre-ticked boxes authorizing the use of cookies did not constitute valid consent. In order for consent to be lawfully obtained to place cookies, active behavior clearly demonstrating consent became necessary. As a result, obtaining consent through inaction or action without any intention of giving consent such as by informing users that their consent is assumed by their continued use of the website is clearly insufficient.

The EDPB quite recently provided further guidance on consent with regard to the use of cookies, in its Guidelines on Consent adopted on 4 May 2020. According to the European body, for consent to be freely given as required under the GDPR, access to services and functionalities must not be made conditional on the user's consent to the storage of information (so called cookie walls). Where there is no possibility for a user to access the content of a website without accepting cookies, it would be deemed that the user's consent is not freely given. The EDPB further clarifies that merely continuing the ordinary use of a website is not conduct from which one can infer an indication by the user of signifying his or her agreement to the processing of information. Controllers must therefore ensure that consent mechanisms are designed in ways that are clear and unambiguous to individuals. Hence, actions such as scrolling or swiping through a webpage or similar user activity may not under any circumstances satisfy the requirement of a clear and affirmative action.

On another note, the Greek supervisory authority fined a local entity of one of the 'Big Four firms' after the data protection authority found that the company failed to ensure lawful, fair and transparent processing of its employees' personal data by relying on the legal basis of consent.[13] The Greek authority claimed that such deemed consent was not a valid lawful basis for processing the employees' data, since consent of data subjects in the context of employment relations cannot be regarded as freely given due to the clear imbalance between the parties. The relevant legal basis for processing employees' information would have been performance of the employment contracts, compliance with a legal obligation or effective operation of the company as part of its legitimate interests.

Right to be forgotten

In the Google v. CNIL case,[14] the ECJ's decision clarifies that, while EU residents have the legal right to be delisted from search results, this right is limited to the borders of the 28 Member States. Although the Court did set limits on the territorial scope of an individual's right to be forgotten in its judgment, it also opened the possibility for national data protection authorities to enact laws with regard to global delisting.

Joint controllership

Under the GDPR, the boundaries between data controllers and processors are somewhat opaque and this tends to make contract negotiations rather complex and time-consuming. In the Fashion ID case,[15] the ECJ adopted a broad scope of joint controllership by declaring that a website operator embedding the well-known 'Like' social plugin can be considered to be a controller jointly with Facebook. Hence, the website operator is also directly responsible for compliance with legal obligations applicable to a controller, including requesting consent and notifying its users prior to the transfer of their personal data to Facebook. The Court further clarified that the website operator's liability as a data controller is limited however to the collection and transfer of personal data to Facebook.

[12] CJEU Case C-673/17, Judgment of the Court of 1 October 2019
[13] Hellenic Data Protection Authority's decision No. 26/2019
[14] CJEU Case C-507/17, Judgment of the Court of 24 September 2019
[15] CJEU Case C-40/17, Judgment of the Court of 29 July 2019

ROOM FOR IMPROVEMENT: BETTER CLARITY AND CONSISTENCY STILL NEEDED

Regardless of the intent to harmonize data protection legislation throughout the European continent, the GDPR may not have completely prevented fragmentation in the implementation of data protection across the EU. The GDPR leaves room for national variations and specifications on several matters such as the age of consent or the processing of sensitive data, leeway which certain EU Member States seem to have deployed to full effect.[16] Furthermore, because of the lack of clarity on certain issues, the national data protection authorities have adopted differing interpretations, guidance and rules. As this may impact businesses operating in several countries across the EU, this fragmentation only serves to magnify the calls for greater certainty and consistency between national legal frameworks.

With regard to overseas transfers of personal data, the GDPR provides a number of tools available for business to lawfully and safely transfer data to third countries and/or international organizations. The first instrument to be relied upon according to the GDPR are adequacy decisions (a list of nations which the EU considers has an adequate level of data protection). Next in line are binding internal corporate rules and standard data protection clauses adopted by the European Commission among others. However, given the limited number of third countries deemed adequate by the Commission, the application of the other tools would clearly benefit from further clarification and guidance as it may be difficult for businesses to determine what may qualify as appropriate safeguards of data protection in terms of overseas transfers.[17]

Emerging technologies constitute new challenges for personal data protection, such as artificial intelligence, block-chain technology and facial recognition. While the GDPR was drafted to be technologically neutral and adequately cover related data protection matters, it appears essential to clarify how the GDPR will apply to emerging technologies in order to avoid restrictive interpretations and to ensure that it can serve as the bedrock on which to develop future digital policy initiatives whilst not hindering innovation.

NON-COMPLIANCE WITH THE GDPR REQUIREMENTS: PENALTIES DEEMED INSUFFICIENT

Under the GDPR, the fines administered by the local data protection regulator are aimed at making non-compliance an onerous and costly mistake for businesses. 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. Additionally, 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 subject rights.

From 25 May 2018 to 17 May 2020, the total GDPR fines across all countries (finalized cases only) reached an aggregate amount of EUR 153 million (approximately USD 167 million).[18] Of note, a third of the total amount of GDPR fines levied have been on Google LLC in January 2019 by the French supervisory authority for violation of the GDPR. This global figure seems quite low given the supervisory authorities' power to administer fines of up to 4% of global annual turnover as mentioned above and it is questionable whether such seemingly 'weak' penalties will have a sufficient deterrent effect on multinational companies.

It is however too early to consider whether GDPR fines will stay in the low range in the future as there remains considerable uncertainty as to the methodology to calculate and impose such penalties. In 2019, the United Kingdom's data protection authority issued two intent-to-fine notices for infringements of the GDPR amounting to GBP 282 million in total (approximately USD 343 million / EUR 314 million), though none of these fines have been finalized yet. Furthermore, according to the German GDPR fining guidelines published in 2019, minor infringements may result in million euro fines. How fines should be calculated under the GDPR remains largely undetermined at this point. Multi-

[16] The National Law Journal, Alston & Bird, 20 June 2018
[17] Note no. 13599/19 of the Council of the European Union regarding the Preparation of the Council position and findings on the application of the GDPR
[18] GDPR Fines Tracker & Statistics, Privacy Affairs, as of 17 May 2020

million euro fines could be more frequent over the coming years but the emergence of a standardized methodology will likely take a long time in coming to fruition.

CONCLUSION

The primary lesson to be drawn from the GDPR's first two years is that consistent implementation of such wide-ranging legislation throughout all EU Member States and compliance of all stakeholders is a dynamic process which cannot magically and seamlessly lock into place. While the legal landscape in Europe and beyond has undoubtedly moved in the direction of more robust personal data protection, close collaboration between European bodies, national data protection authorities as well as businesses and civil society remains crucial to achieving the essence of the GDPR. The European Commission's first report on the evaluation and review of the GDPR, upon its eventual release, will be an invaluable resource to promote harmonization of GDPR enforcement across Europe over the coming years and identify areas where greater collaboration is still wanting.

Differences can indeed be drawn from the approaches taken by the Southeast Asian region with respect to data protection due to the lack of a centralized governing body such as the European Commission, Southeast Asian nations may find it beneficial to try achieving a harmonized approach towards regional data protection. While this is a lengthy process as we can so far gather from the GDPR experience, timely action by Southeast Asian jurisdictions to start bolstering their domestic data protection frameworks and having a regional view of data privacy legislation would clearly be beneficial in terms of prospering from the booming digital economy that exists across Southeast Asia. Inconsistent approaches to data protection rules throughout the region may only hamper such growth in the long run and certain nations may lose out on the attendant opportunities if they do not rapidly put the required regulatory frameworks into effect.

The past two years of GDPR enforcement further illustrates that while EU Member States are entitled to impose onerous fines on the most serious infringements, very few have made use of such cudgels so far. The relevance of these severe penalties for ASEAN countries could be called into question, notably since imposing heavy penalties (as provided under the GDPR) on relevant stakeholders could potentially kill any Asian digital potential in its crib. In any event, the GDPR experience re-affirms that time is of the essence in terms of pursuing a comprehensive regulatory framework across ASEAN states so that they may fully enjoy the opportunities offered by the digital boom while ensuring a high standard of personal data protection to enable safe data flows across the region and other parts of the world.

CONTACTS

Audray Souche
Partner, Thailand Managing Director
audray.souche@dfdl.com

Kunal Sachdev
Regional Senior Legal Adviser, Deputy Head of Regional Banking and Finance Practice
kunal@dfdl.com

Marion Lagrange
Legal Adviser
marion.lagrange@dfdl.com

EXCELLENCE · CREATIVITY · TRUST
Since 1994

BANGLADESH | CAMBODIA* | INDONESIA* | LAO PDR | MYANMAR | PHILIPPINES* | SINGAPORE | THAILAND | VIETNAM

** DFDL collaborating firms*