CLIENT NOTE

WHAT IS THE GDPR AND HOW DOES IT AFFECT MY ORGANISATION?

5 June 2018

For any queries relating to this article,

please contact:

Zechariah J.H. Chan

Partner, Intellectual Property

DID: 6557 4710

zechchan@leenlee.com.sg

Tan Sih Im

Associate, Intellectual Property

DID: 6557 4612

tansihim@leenlee.com.sg

Authors:

Zechariah J.H. Chan

Tan Sih Im

Introduction

1. On 25 May 2018, the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") came into force two years after being approved by the European Union ("**EU**") Parliament in April 2016.

2. The GDPR is the chief regulation on data protection and privacy in the EU. It supersedes and is intended to replace the Data Protection Directive 95/46/EC and to harmonize data privacy laws across Europe.

Relevance of the GDPR to Singapore organisations

Applicability of the GDPR

3. Although the GDPR is a piece of European legislation, its intended extra-territorial reach means that it remains relevant to Singaporean businesses and/or organisations. In particular, Article 3(2) of the GDPR provides that:

> "*This Regulation applies to the processing of personal data of **data subjects who are in the Union by a controller or processor not established in the Union**, where the processing activities are related to:*
>
> *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to **such data subjects in the Union**; or*
>
> *(b) the monitoring of their behaviour as far as their **behaviour takes place within the Union**.*" (emphasis added)

4. This effectively means that organisations that are not established in the EU would still be required to comply with the GDPR insofar as they process the personal data of individuals in the EU and these processing activities relate to:

About us

For more legal updates, please visit the News & Publication Section of Lee & Lee's website at www.leenlee.com.sg or follow Lee & Lee's facebook page at www.facebook.com/leenlee.com.sg/

(a) the offering of goods or services to individuals in the EU; or

(b) the monitoring of the behaviour of individuals in the EU taking place within the EU.

5. Given the broad wording of Article 3(2), it would appear that the GDPR would extend to cover situations such as a Singaporean e-commerce company offering goods or services through its website to individuals in the EU, or a Singapore company tracking the behaviour of individuals in the EU to create profiles of them.

"Offering of goods or services"

6. While there has yet to be any judicial determination on what constitutes an "*offering of goods or services*" to individuals in the EU, the GDPR does offer some guidance. For instance, Recital 23 of the GDPR provides that the test for determining this issue is:

> "*whether it is apparent that [the organisation] envisages offering services to data subjects in one or more Member States in the Union*".

7. Recital 23 also offers assurance that the mere accessibility of the organisation's website or contact details in the EU or the use of a language generally used in the third country where the organisation is established would generally be deemed insufficient in establishing an intention to offer goods or services to individuals in the EU.

8. Further, Recital 23 also lists the following as factors which would militate towards a finding that an organisation "*envisages offering goods or services to data subjects in the Union*":

(a) the 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

(b) the mentioning of customers or users who are in the Union.

9. It is crucial to note also that Article 3(2) has been specifically worded to capture the offering of goods or services without payment. Therefore, non-profit organisations are also potentially liable under the GDPR.

Processing personal data on behalf of a controller

10. Even if an organisation does not offer goods or services directly to individuals in the EU, the GDPR may still be relevant if that organisation processes personal data on behalf of a controller subject to the GDPR, *i.e.* if the organisation is a "processor" under the GDPR. In particular, Article 28(1) provides that:

> "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet*

the requirements of this Regulation and ensure the protection of the rights of the data subject."

11. Article 28 also sets out obligations that the processing of personal data by a processor must be subject to under "*contract or other legal act under Union or Member State law*". This means that Singapore organisations which process personal data on behalf of controllers subject to the GDPR would also have to ensure that they are GDPR-compliant.

Touchstones of the GDPR

12. The GDPR lays down touchstones underlying the processing of personal data under the GDPR. Article 5 provides that personal data shall be:

    (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

    (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");

    (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

    (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");

    (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation"); and

    (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

13. Further, a data controller must be responsible for and able to demonstrate compliance with the above principles ("accountability").

14. The GDPR also enshrines the following individual rights:

    (a) the right of access to an individual's personal data and information concerning the processing of such personal data;

    (b) the right to rectification of inaccurate personal data concerning an individual;

    (c) the right to erasure of personal data concerning an individual's;

    (d) the right to restriction of processing in circumstances such as where the accuracy of the personal data is contested or where the processing is unlawful;

    (e) the right to data portability;

    (f) the right to object to processing of an individual's personal data in prescribed circumstances; and

    (g) the right not to be subject to automated individual decision-making (including profiling) which has legal effects on an individual or significantly affects that individual.

Noteworthy differences between the PDPA and GDPR

15. As evident from Paragraphs 12 to 14 above, there are similar concepts in both the GDPR and PDPA, *e.g.* the accuracy obligation and the right to access. However, organisations should be aware that there are fundamental differences in the two pieces of legislation such that compliance with the PDPA would not necessarily mean that an organisation is GDPR-compliant.

16. The following paragraphs outline several noteworthy provisions in the GDPR which are markedly different from the equivalent requirements under the PDPA.

Mandatory data breach notification

17. Whereas the PDPA does not presently prescribe any mandatory data breach notification requirement and merely recommends voluntarily notification where sensitive personal data is involved, the breach might cause public concern and/or where there is a risk of harm to a group of affected individuals, the GDPR imposes a positive duty on a data controller to notify:

(a) the supervisory authority without undue delay and, where feasible, not later than 72 hours of becoming aware of a data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals; and

(b) affected individuals without undue delay, where the personal data breach is likely to result in a high risk to the rights and freedoms of such individuals.

18. A data processor is also required to notify its data controller without undue delay after becoming aware of a breach.

Special categories of personal data

19. Another key difference between the PDPA and the GDPR is their respective treatments of special categories of personal data.

20. Although the PDPC has previously issued guidelines that certain types of personal data (*e.g.* financial or health information) are more sensitive and should therefore be accorded a higher standard of care, it does not contain explicit categorisations of personal data. Indeed, as a general rule, the collection, use, and disclosure of all types of personal data are subject to the same data protection provisions under PDPA (although the standard of care expected of organisations might vary with the sensitivity of the personal data at stake).

21. On the other hand, unless statutory exceptions apply, Article 9 of the GDPR explicitly prohibits the:

> *"[p]rocessing of **personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership**, and the processing of **genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation**". (emphasis added)*

22. One of the exceptions to this general prohibition is "explicit consent" to the processing of such special categories of personal data, and even then, such consent may be invalid if the EU or the applicable laws of an EU Member State provides that the Article 9 prohibition may not be lifted by the individual. Indeed, this represents considerably stricter rules governing the processing of sensitive personal data under the GDPR as compared to the PDPA.

Consent

23. The requirement to obtain consent for the processing of personal data is also arguably more onerous under the GDPR than the PDPA.

24. The PDPA requires organisations to obtain valid consent from the individual for the collection, use, or disclosure of his personal data ("**Consent Obligation**"). However, the mode of obtaining consent is not statutorily prescribed. Whilst the PDPC encourages

organisations to obtain consent through a positive action of an individual, a failure to opt out could technically constitute consent under the right circumstances.

25. On the other hand, "consent" is specifically defined in the GDPR as:

> "***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*". (emphasis added)

This would mean that as a general rule, the GDPR strictly prohibits the obtaining of consent through an opt-out method.

26. Further, under the PDPA an individual may be deemed to have consented to the collection, use or disclosure of his personal data even if he has not actually given consent if:

    (a) he voluntarily provides his personal data for a purpose and it is reasonable that he would do so; or

    (b) he gives or is deemed to have given consent for disclosure of his personal data by organisation A to organisation B for a purpose.

27. On the other hand, the concept of "deemed consent" does not appear to be provided for in the GDPR.

Data protection officer

28. All organisations subject to the PDPA are required to appoint a data protection officer ("**DPO**") for ensuring the organisation's compliance with the PDPA.

29. On the other hand, an organisation is only required to appoint a DPO under the GDPR if the core activities of the organisation consist of:

    (a) processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or

    (b) processing on a large scale of special categories of data (discussed in Paragraph 21 above) and personal data relating to criminal convictions and specified offences.

30. Further, while the PDPA does not prescribe the selection criteria for a DPO, the GDPR requires that the DPO be selected "*on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the [following] tasks*":

    (a) informing and advising the organisation and its employees of their obligations under the GDPR and other EU or Member State data protection provisions;

    (b) monitoring compliance with the GDPR and EU or Member State data protection provisions and with the data protection policies of the organisation;

(c) providing advice as regards data protection impact assessment and monitoring its performance;

(d) cooperating with the supervisory authority; and

(e) acting as the contact point for the supervisory authority on data processing issues.

Penalties for non-compliance of the GDPR

31. The consequences of non-compliance with the GDPR are significant. The GDPR provides for the imposition of fines of up to:

(a) **10,000,000 euros or 2% of the total worldwide annual turnover** of the preceding financial year (whichever is higher) for more minor infringements of the GDPR (*e.g.* failure to satisfy the conditions applicable to obtaining a child's consent in relation to information society services, failure to implement technical control or data protection by default, or failure to notify breaches); or

(b) **20,000,000 euros or 4% of the total worldwide annual turnover** of the preceding financial year (whichever is higher) for more major infractions (*e.g.* for violations of the basic principles for processing, including conditions for consent, set out in the GDPR, and infringements of the regulations regarding the transfer of personal data to a third country or an international organisation).

32. By way of contrast, the maximum financial penalty that the Personal Data Protection Commission ("**PDPC**") is allowed to impose on an organisation to is S$1 million.

Conclusion

33. Insofar as an organisation is processing data in Singapore and falls within the ambit of Article 3(2) of the GDPR, it would have to comply with both the PDPA and GDPR concurrently.

34. Given the substantive differences between the respective requirements under the PDPA and GDPR as discussed in Paragraphs 15 to 27 above (with the GDPR arguably containing more stringent requirements) and the significant penalties that may be imposed under the GDPR, organisations which do have a presence in the EU should exercise extra caution to ensure that they are GDPR-compliant since a judgment obtained there could be enforced against them in the EU.

35. We would advise organisations to examine the applicability and relevancy of the GDPR to their businesses and/or operations and, if the GDPR is applicable, to seek legal advice on such compliance.

About Lee & Lee

Lee & Lee is one of Singapore's leading law firms being continuously rated over the years amongst the top law firms in Singapore. Lee & Lee remains committed to serving its clients' best interests, and continuing its tradition of excellence and integrity. The firm provides a comprehensive range of legal services to serve the differing needs of corporates, financial institutions and individuals. For more information: visit www.leenlee.com.sg.

The following partners lead our departments:

Kwa Kim Li
Managing Partner
kwakimli@leenlee.com.sg

Quek Mong Hua
Litigation & Dispute Resolution
quekmonghua@leenlee.com.sg

Owyong Thian Soo
Real Estate
owyongthiansoo@leenlee.com.sg

Tan Tee Jim, S.C.
Intellectual Property
tanteejim@leenlee.com.sg

Adrian Chan
Corporate
adrianchan@leenlee.com.sg

Louise Tan
Banking
louisetan@leenlee.com.sg