LHAG CELEBRATES 25TH ANNIVERSARY

Legal Herald

JUNE 2018

in this issue

GDPR and the Malaysian Business

by Kelly Yeo Chei Jun

In the wake of allegations surrounding a data breach involving Cambridge Analytica and information relating to 50 million Facebook users, much talk and focus has been placed on the gaps in the protection of an individual's privacy in the sphere of the internet. Attention has also been turned towards new data protection rules of the European Union (EU) which take effect this month and the plausibility of such rules affording greater protection to individuals in the digital age.

In the EU, the Data Protection Directive[1] governs the protection of an individual's personal information. Since being passed in 1995, the Data Protection Directive has not been updated to account for advancement in technologies where increasingly vast amounts of data can be easily and rapidly processed and transferred across borders. Further, directives in the EU lay down results that must be achieved by each Member State, the implementation of which may not be the same in each Member State and may be open to interpretation.

1 Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC)

KDN PP 12853/07/2012 (030901)

Printed by Percetakan Jiwabaru Sdn. Bhd.
No. 2, Jalan P/8, Kawasan MIEL Fasa 2, Bandar Baru Bangi, 43650 Bangi, Selangor Darul Ehsan, Malaysia

With the aim of strengthening the data protection of individuals in the EU and promoting the digital single market with unified rules on data protection, the General Data Protection Regulation (GDPR)[2] was issued by the European Parliament in April 2017. The GDPR, which took effect on 25 May 2018, replaces the Data Protection Directive. Regulations in the EU have binding legal force throughout every Member State on the implementation date.

KEY CONCEPTS

Data controller or **controller** (known as a "data user" in Malaysia) is the person who determines the purposes and means of processing of personal data

Data subject: the individual who is the subject of the personal data

Malaysian businesses and the GDPR

One feature of the GDPR that has been the topic of much discussion is its extra-territorial application to data users who are not situated in the EU.

Though the GDPR is a piece of European legislation, it may apply to non-EU established organisations, if the organisation either:

(1) processes the personal data in the context of activities of an establishment in the EU; or

(2) processes the personal data of individuals in the EU or targets to monitor activities of individuals in the EU where such processing activities of personal data of such organisation is related to:

(a) the offering of goods and services to individuals in the EU (whether consideration is involved or not); and

(b) the monitoring of behaviour of individuals in the EU, in so far as their behaviour takes place in the EU.[3]

Offering of goods and services

The Recitals of the GDPR provide certain factors that indicate whether an organisation would be deemed to be "*offering goods and services*" to individuals in the EU. Among the factors indicated are:

(1) Language: Usage of language generally used in Member States and the possibility of ordering goods in such language;

(2) Currency: Usage of currency of Member State (e.g. euro);

(3) Delivery to the EU: Physical goods will be delivered to a Member State;

(4) Customer base: A large proportion of customers is based in the EU or there is mention of customers or users who are in the EU; and

(5) Targeted advertising: There are paying adverts to target individuals in a Member State.

Monitoring behaviour of individuals in the EU

Organisations should also note that profiling of EU individuals over the internet by tracking and collecting

2 Regulation (EU) 2016/679 of the European Parliament and 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

3 GDPR, Art 3(2)

information relating to an individual and subsequently analysing or predicting the individual's personal preferences, behaviours and attitudes would be deemed to be "*monitoring behaviour of individuals in the EU*".

Malaysian businesses as data processors

Prior to the GDPR, data processors did not have direct liability under the Data Protection Directive. Compliance with data protection laws is the responsibility of the data controller. Further, data controllers were required to enter into data processing agreements with data processors, but the Data Protection Directive does not specify the contents or requirements with regard to such an agreement.

The GDPR imposes obligations upon data processors indirectly and/or directly. This is done by way of stipulating, in the GDPR, specific requirements to be set out in a written arrangement or contract between a data controller and a data processor — for instance, that a data processor is not to engage a sub-processor without the prior written authorisation of the controller.[4] Certain obligations are imposed directly upon the data processor; for instance, the requirement to comply with provisions on security of processing under the GDPR.[5]

Even if Malaysian businesses are not "*offering goods or services*" or "*monitoring behaviour*" of data subjects in the EU, businesses acting as data processors to their European counterparts should similarly take note of the developments under the GDPR. This is because their European counterparts are required to impose such obligations under the GDPR on data processors with whom they have arrangements for data processing activities.

Requirements under the GDPR

In Malaysia, the protection of an individual's personal data is governed under the Personal Data Protection Act 2010 (PDPA). Though not identical, parallels can be drawn in interpreting the data protection principles under the PDPA with data protection principles under the Data Protection Directive and the UK's Data Protection Act 1998.

The definition of personal data under the PDPA is similar as that provided for under the GDPR. The PDPA, however, only applies to personal data processed pursuant to a commercial transaction, whereas there is no such limitation upon the application of the GDPR.

(i) Consent

Consent is an integral requirement under both the PDPA and the GDPR. The PDPA, however, does not define what consent entails. Further regulations provide that consent collected has to be in a form that can be maintained by the data user and any consent obtained should be presented distinguishable in its appearance from such other matter.[6] The data user should also ensure records of consent collected are maintained as the PDP Commissioner has the power to inspect such records at any time.[7]

4 *Ibid*, Art 28(2)
5 *Ibid*, Art 28(3)(c)
6 Personal Data Protection Regulations 2013
7 PDPA, s 44 and PDP Regulations, reg 14

Under the GDPR, "consent" has to be freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or a clear affirmative action. This would seem to indicate that the opt-out method of obtaining consent may not fall within this definition.

As a comparison, in Malaysia, the collection of consent by way of "opt-out" method is specifically permitted under certain circumstances. Specific industry codes of practice (i.e. banking and insurance) have provided that an "opt-out" method of collection of consent with regard to direct marketing of the data user's products is allowed.[8]

(ii) Representative in the EU

For non-EU businesses that process personal data of EU customers, whether in the context of offering goods and services or monitoring the behaviour of such data subjects, the GDPR requires the non-EU business in question to designate a representative based in the "*main establishment*" of such non-EU business located in the Member State who will act as the point of contact for the relevant data protection authority.

(iii) Data Protection Officer

Under the GDPR, certain organisations processing personal data (whether in the capacity of a data controller or a data processor) are required to specifically appoint a data protection officer. For example, organisations whose core activities involve the regular and systematic monitoring of data subjects on a large scale. The role and obligation of such data protection officer are stipulated in the GDPR; this includes acting as a liaison to data subjects with regard to all issues relating to the processing of their personal data.

Although data users in Malaysia are required to identify a contact person in a data protection notice, for data subjects to contact, there is no requirement for a specific position of a data protection officer under the data protection regime in Malaysia.

(iv) Data breach and reporting obligations

Pursuant to the GDPR, data controllers are obliged to report data breaches to the relevant supervising authority in their Member State within 72 hours. Data controllers are also required to report such a breach to the relevant data subjects if the result of the breach is likely to result in a high risk to the rights of the data subject.

In Malaysia, the PDPA does not impose an obligation upon data users to report to the PDP Commissioner when a data breach occurs, let alone notify the data subject in question.

Rights of data subject

The GDPR affords better protection of the rights of data subjects. The rights of data subjects recognised under the GDPR include:

(i) Right to be forgotten/right to erasure

When a data controller receives a request to erase personal data belonging to the data subject in question, the data controller has to comply with the request without undue delay (save where the situation falls within an exemption provided for under the GDPR).[9]

In Malaysia, there is no clear equivalent of a right to be forgotten or right to erasure though Malaysian data subjects may withdraw consent for the processing of his

8 Paragraph 14 of the Code of Practice on Personal Data Protection for the Insurance and Takaful Industry in Malaysia and para 4.10 of the Code of Practice on Personal Data Protection for the Banking and Financial Sector

9 GDPR, Art 17

or her personal data. There is little guidance on the effect of such withdrawal, but the exercise of such right may result in the data user having to delete the personal data of the data subject in question.

(ii) Data portability

Data subjects are given a right under the GDPR to request that their information held by a data controller be provided in a machine readable form. Further, data subjects may request that their personal data be transmitted from one data controller directly to another. This right applies where the processing is:

(a) based on the data subject's consent or where the processing is carried out pursuant to the performance of a contract; and

(b) where the processing is carried out by automated means.[10]

In Malaysia, data subjects have a right to request for their information from a data user, but there is no specific provision on the method or the medium in which such records of personal data is to be given. The PDPA further does not provide for a right for data subjects to request transfer of personal data to different data users.

Conclusion

Although there are questions and uncertainties on the practicability of enforcing the GDPR outside the EU, Malaysian businesses should note that failure to comply with the GDPR could result in fines (civil penalties) up to the higher of 20 million euros or 4% of the organisation's global turnover. Taking into account the heavy penalties and potential reputational damage (in particular those with multi-jurisdiction presence), Malaysian businesses should not be so quick to discount compliance with the GDPR.

Steps should be taken to assess whether the GDPR would be applicable to their business and processes and policies that are compliant with the GDPR should be implemented. **LH-AG**

About the author

Kelly Yeo Chei Jun (ycj@lh-ag.com) is an associate with the TMT Practice, and is part of a team headed by Adlin Abdul Majid.

Adlin Abdul Majid (aam@lh-ag.com) is a partner in the TMT Practice and also heads the Regulatory & Compliance team.

10 *Ibid,* Art 20