LAW GAZETTE

FEATURE - May 2018

The New European General Data Protection Regulation

7 min read
by Sebastian Blasius

Why Singapore Businesses May Have to Comply with More than Just Their National Personal Data Protection Regime

On 25 May 2018 the European General Data Protection Regulation (**GDPR**) *will come into force. Due to its unlimited territorial scope, many deem this day to be the start of a new era in the field of worldwide personal data protection. Given the possibility of high financial penalties, decision makers are well advised to determine in time whether the GDPR is relevant for their businesses and what measures have to be implemented to be compliant.*

Laws to protect personal data were for the longest time non-existent in most South East Asian countries. With the coming into force of the Singapore Personal Data Protection Act (**PDPA**) in 2014, this situation has changed. Continuous efforts of the Personal Data Protection Commission (**PDPC**), such as advertising campaigns or letters addressed to individual businesses, have led to an enhanced awareness of personal data protection laws. Yet, the number of cases in which the PDPC imposes financial penalties on organisations for non-compliance with the data protection rules keeps on growing. This shows that many organisations still struggle to adapt to the new rules or, sometimes to avoid costs, consciously choose to ignore them.

The European General Data Protection Regulation, which will be in force from 25 May 2018, will subject many businesses in Singapore to additional data protection laws. This increases their administrative burden substantially. Even businesses that are already compliant with the PDPA may have to implement additional measures to take the often stricter rules of the GDPR into account. The financial penalties possible in case of non-compliance with the GDPR — more than €20 million — take this topic to a whole new level.

This article aims to provide readers with a first overview of the impact the GDPR may have on their business. It starts with some general comments on the GDPR (see part 1) and provides an overview about the situations in which the GDPR may be relevant for Singapore business organisation (see part 2). Afterwards, it describes the GDPR's key principles relating to the processing of personal data (see part 3) and the rights the regulation grants

to individuals (see part 4). Part 5 covers the obligation to appoint a data protection officer and a representative in the European Union. Possible sanctions in case of an infringement of the GDPR's provisions are described in part 6.

General Notes on the GDPR

The European "Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" — short: General Data Protection Regulation or GDPR — governs the processing of personal data. "Personal data" is all information related to an identified or identifiable human being. "Processing" refers, roughly speaking, to everything that is done with this personal data, most important its collection, use and disclosure. The GDPR does hence present an exhaustive protection regime for personal data.

It has, first of all, effect on personal data processed by European organisations. However, where a sufficient connection to the EU can be established, the GDRP will as well be relevant for non-European business organisations. Hence, many deem its coming into effect to be the start of a new era in the field of worldwide personal data protection.

The GDRP's Relevance for Singapore Organisations

Cases in Which the GDPR is Relevant for Singapore Business Entities Because of Their Activities

First and foremost, the GDRP applies to the processing of personal data by organisations established in the European Union. However, when personal data of persons who are in the European Union is processed, the regulation may also be relevant for Singapore business entities.

If the respective data processing activities are **related to the offering of goods and services to persons in the EU** (irrespective of whether a payment is required or not) the provisions of the GDRP have to be abided by. All circumstances of a particular case should be taken into account in order to determine whether or not this is the case. Examples of relevant factors are the language of an offer, the currency which is accepted as payment for goods and services offered or the existence of an option to send goods to the EU or to render services in the EU.

The second case in which the GDRP applies is when the data processing activities **are related to the monitoring of persons' behaviour taking place within the EU**. This may especially be the case, where a person is tracked on the internet (which relates in particular to web tracking via cookies or social plug-ins).

The Transfer of Personal Data from Europe to South East Asia

Singapore companies do often have European parent companies or are part of a bigger International group of companies. Not seldom, personal data is transferred from European group companies to their Asian affiliates. Especially in this case, caution is advised and the new laws have to be taken into account.

Generally speaking, a transfer to a — from a European perspective — "third country" is only allowed:

1. If the European Commission has made a decision on the adequacy of the protection of personal data in that particular third country ("**adequacy decision**");
2. If the transferring organisation has put appropriate data protection safeguards in place; or
3. If one of the narrow exception clauses of the GDRP applies.

The same goes for data transfers from one third country (to which data from the EU was transferred) to another third country.

With regard to South East Asian states, the Commission has so far not made any adequacy decision. Hence, if a European organisation would like to transfer personal data to its Singapore subsidiary and no exception is applicable, it has to provide for appropriate safeguards. The same applies if the subsidiary transfers personal data to another "third country". Such safeguards may especially be put in place via the implementation of binding corporate rules in a group of companies or contractual clauses between the transferring and the receiving organisation.

Key Principles of the GDPR

To the extent the GDPR applies to the data processing activities of an organisation, especially the following six key principles have to be taken into account:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the individual concerned ("**principle of lawfulness, fairness and transparency**"). The GDPR lists a number of cases in which data processing is lawful. First and foremost, this is the case if consent is given by the individual to the processing of his personal data for a specific purpose. While this is a familiar principle in many jurisdictions, the range of information which has to be provided to an individual, when collecting personal data from it, does substantially exceed the requirements under most national personal data protection laws. Not only do organisations have to provide information about the purpose of the data processing for which the personal data is intended. They are, for example, also required to inform individuals about the legal basis for the data processing or, if applicable, the intention to transfer data to a third country and the means by which data is safeguarded in this respect. Furthermore, information about the storage period and certain rights of the individuals in relation to their personal data may have to be provided.

2. Personal data shall only be collected for specified, explicit and legitimate purposes. It shall not be processed in a manner that is incompatible with these purposes ("**principle of purpose limitation**").

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which the personal data is processed ("**principle of data minimisation**").

4. Personal data shall be accurate and, where necessary, kept up to date. Organisations must take all reasonable steps to make sure that personal data which is inaccurate (in relation to the purpose for which it is processed) gets erased or rectified without delay ("**principle of accuracy**").

5. Personal data shall in general be kept in the form which permits the identification of an individual for no longer than is necessary for the purposes for which the personal data is processed ("**principle of storage limitation**").

6. Personal data shall be processed in a manner that ensures its appropriate security ("**principle of integrity and confidentiality**"). This does especially include appropriate protection against unauthorised or unlawful

processing and against accidental loss, destruction or damage.

In addition to these key principles, business entities have to take into account that the processing of certain categories of personal data is generally prohibited. This includes, for example, data revealing the racial origin or religious belief of a person or data concerning a person's sexual orientation.

Furthermore, organisations have to implement technical and organisational measures to ensure an appropriate level of security with regard to the processing of personal data. In case of a personal data breach, the responsible supervisory authority (and possibly also the individual concerned) will generally have to be informed without undue delay and, where feasible, not later than 72 hours after an organisation became aware of the personal data breach.

How Partners, Customers and Other Individuals Can Hold a Business Entity Accountable

The GDPR grants several rights to individuals. Organisations are under an obligation to facilitate the exercise of these "data subject rights" and to provide information on the action they take on the exercise of these rights by an individual. In particular, individuals may have:

1. The right to access the personal data processed by organisations and to be provided with certain information pertaining hereto ("**right of access**");
2. The right to have inaccurate personal data rectified and to have incomplete personal data completed ("**right to rectification**");
3. The right to have personal data erased ("**right to be forgotten**");
4. The right to restrict the processing of personal data ("**right to restriction of processing**");
5. The right to receive the personal data, which they have provided to an organisation, in a structured, commonly used and machine-readable format and to a transmittance of this data to a third party ("**right to data portability**");
6. The right to object to processing of personal data ("**right to object**"); and
7. The right not to be subject to a decision based solely on automated processing which produces legal effect concerning the individual or similarly significantly affects it ("**right not to be subject to automated decision-making**").

The Data Protection Officer and the "Representative in the European Union"

Data Protection Officer

Pursuant to the terms of the GDPR, many business entities will have to appoint a data protection officer (**DPO**). Broadly speaking, an organisation will have to appoint a DPO if its core activities consist of processing operations

which require regular and systematic monitoring of persons on a large scale. Furthermore, a DPO will be necessary if the core activities of an entity consist of processing special categories of data (such as data revealing the racial or ethnic origin, religious beliefs, biometric data or data relating to criminal convictions/offences) on a large scale.

The DPO's main responsibility is the monitoring of his organisation's compliance with the GDPR. While the DPO may be a staff member, organisations are also free to appoint external advisors on the basis of a service contract.

Representative in the EU

If a company established outside the EU falls within the GDPR's scope of application, it must appoint a so-called "representative in the Union". This representative has to be established in one of the EU member states where the individuals whose personal data is processed are. The representative shall be a point of contact for individuals and/or supervisory authorities with regard to GDPR related questions. Exceptions from the obligation to appoint a representative may apply, if data processing is only occasional and does not involve particularly sensitive data on a large scale.

What Happens if an Organisation Does Not Comply with the GDPR?

In case of an infringement of the provisions of the GDPR, high administrative fines are possible. Depending on the infringed provision, these fines can amount up to €20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Conclusion

While Singapore businesses still struggle to implement the procedures necessary under the PDPA, the GDPR may soon make many of them subject to an even stricter data protection regime. Given the possibility of high financial penalties, decision makers are well advised to determine in time whether the GDPR is relevant for their businesses and what measures have to be implemented to be compliant.

Tags: DATA PROTECTION, GDPR, GENERAL DATA PROTECTION REGULATION, PDPA, PERSONAL DATA