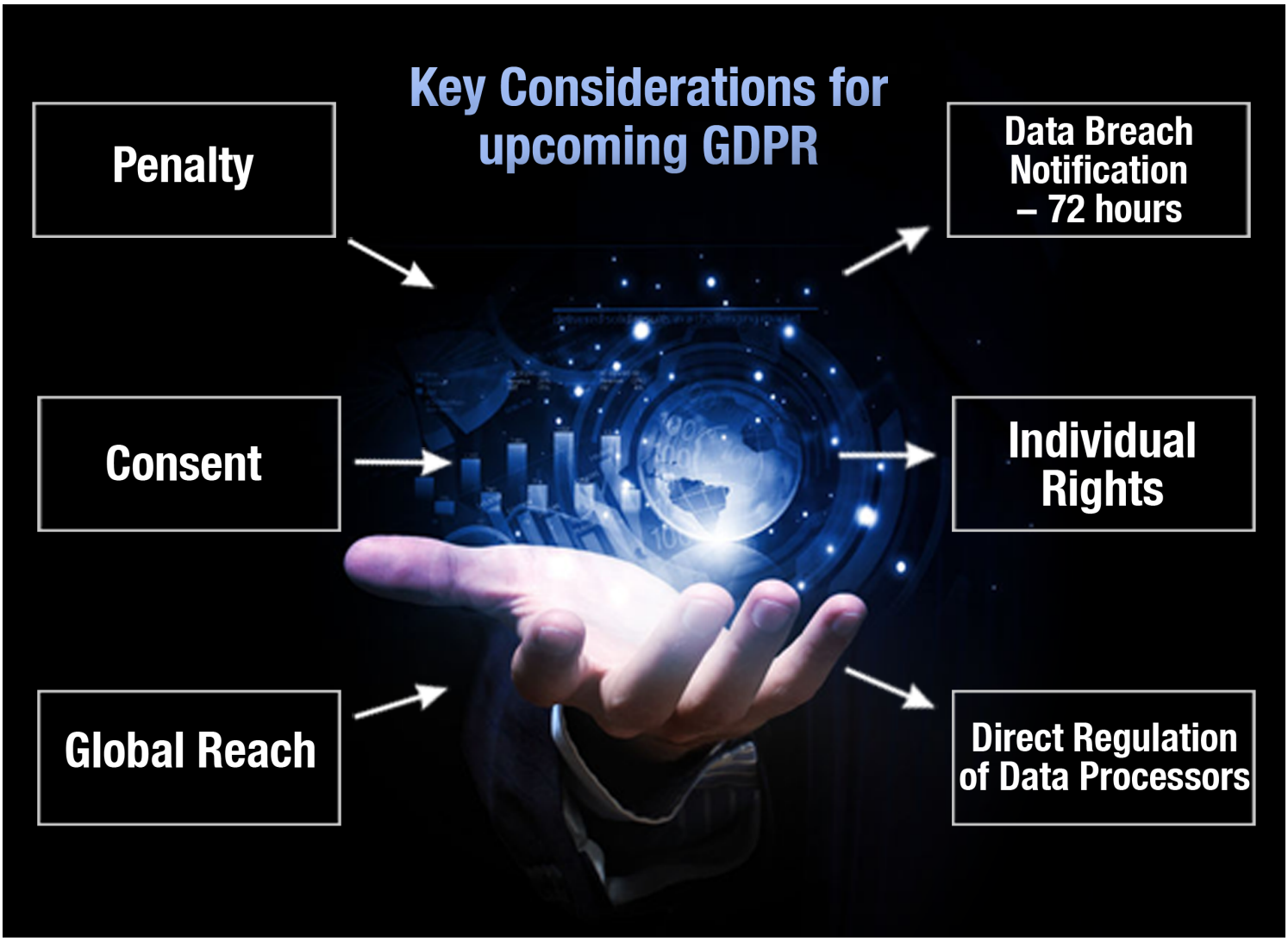
# COMPLIANCE WITH THE GDPR IN SINGAPORE

*Posted on May 24, 2018*

**Category:** CNPupdates




**Date Published: 24 May 2018**

**Authors and Contributors: Wong Pei-Ling, Martin Hemmer, Randall Perera, and Vitoria Owyong.**

This article is written in conjunction with **AKD Benelux Lawyers**, a Dutch law firm recently named Benelux law firm of the year 2018.

# Introduction

The European Union ("**EU**") General Data Protection Regulation (the "**GDPR**") was adopted on 14 April 2016 and will come into force on 25 May 2018. The GDPR is an ambitious piece of legislation, unifying data protection laws across the EU and, purporting to have a global reach in protecting the personal data of EU citizens.

With stringent new requirements, the GDPR applies to all organizations outside of the EU as long as the

organization:

1. offers goods or services to individuals in the EU irrespective of whether a payment is required; or
2. monitors the behaviors of individuals within the EU,

with potentially hefty penalties of up to 20 million EUR or 4% worldwide annual turnover of the preceding year (whichever is higher) for the infringement of provisions under the GDPR.
The GDPR's requirements are more rigorous than that of Singapore's own Personal Data Protection Act 2012 ("**PDPA**"). Organizations whose systems and procedures currently comply with the PDPA may nevertheless be in danger of falling afoul of the GDPR. We elaborate on the key features of this enhanced regime below.

In summary, organizations need to ensure that their internal processes and policies comply with the following requirements:

1. Consent obtained from data subjects for the processing of his/her personal data is clear and unambiguous. The purpose of obtaining such personal data should be clearly stated;
2. Personal data should not be retained longer than is necessary for the purposes for which the personal data was processed;
3. Data subjects should have the right to:
    - access and correct personal data concerning him/her;
    - withdraw consent to the processing of his/her personal data at any time, and such withdrawal of consent should be as easy to withdraw as it is to give;
4. No processing of personal data classified as 'special' under the GDPR (i.e. racial, ethnic origin, sexual orientation, philosophical beliefs) unless the limited exemptions under Article 9(2) of the GDPR applies; and
5. Personal data breaches should be reported no later than 72 hours from the time the breach is discovered. Additionally, the breach and any subsequent remedial actions have to be clearly documented;

# The GDPR's Global Scope

Presently, the PDPA applies only if the data was collected, used or disclosed in Singapore (it is irrelevant if the organization is located in Singapore).
The GDPR has no such geographical restriction. All organizations globally will have to comply with the GDPR as long as the organization:

1. offers goods or services to individuals in the EU, irrespective of whether a payment is required; or
2. monitors their behaviors within the EU.

The PDPA also provides exemptions from data protection obligations to the following entities:

1. individuals acting in a personal or domestic capacity;
2. employees acting in the course of his/her employment with an organization;
3. public agencies;
4. any organization acting on behalf of a public agency in relation to the collection, use or disclosure of personal data; or
5. organisations that are data intermediaries are also partially excluded from the provisions under the PDPA.

By contrast, the GDPR applies so long as an individual or entity (including a public authority or agency) falls within the definition of '*data controller*' or '*data processor*' under Article 4 of the GDPR, save that natural persons acting "*in the course of a purely personal or household activity*" are exempted.

This is particularly significant in relation to data processors, third parties that collect and process data on behalf of other organizations (who fall under the definition of '*data intermediaries*' under the PDPA and enjoy wide exemption from data protection obligations). Both data controllers and processors are subject to the provisions of the GDPR. The GDPR now imposes direct obligations making data processors liable for data protection infringement.

Organizations should note the applicability of the GDPR in Singapore, particularly if its businesses are aligned with the above conditions. This is relevant particularly in light of the severe penalties which the EU may impose for data breaches, as discussed in the following section.

# Penalties

Under the PDPA in Singapore, different administrative fines are applicable to both individuals and organizations. The GDPR makes no such distinction. The definitions of the data controller and data processors under the GDPR include individuals, organizations or other legal entities, and even public authorities and agencies. All are subject to the same stringent penalties under the GDPR.

Under the PDPA, depending on the provision infringed, penalties for organizations will not exceed S$50,000 or S$100,000, as the case may be. Penalties for individuals will not exceed S$5,000 or S$10,000, as the case may be, although in egregious breaches there is a discretion to also impose a term of imprisonment of up to 12 months or 3 years as the case may be.
However, under the GDPR, depending on the provision infringed, entities may be subject to fines of up to 20 million EUR or 4% of a worldwide annual turnover of preceding financial year (whichever is higher) may be imposed on the individual or organization.

Given the intended global reach of the GDPR, it is therefore imperative that organizations (particularly those which do business in the EU) take precautions to ensure that they are compliant with the provisions of the GDPR. This may also apply where the business of an organization is to process personal data on

behalf of other third parties, where the existing regulations under the PDPA are fairly light in comparison.

## Consent

Consent has previously been seen as an absolute defense to privacy infringements. This changes with the GDPR.

Whilst the PDPA prohibits organizations from collecting, using or disclosing a data subject(s)' personal data unless the data subject(s) gives his/her consent for the collection, use or disclosure of his/her personal data, there are a number of situations where a data subject(s) is deemed to have given her/her consent. In addition, there are broad exemptions under which organizations are not required to obtain consent from data subject(s) under the PDPA. For instance where, (i) personal data is publicly available; (ii) the use of personal data is necessary for any investigation or proceedings by the organization; or (iii) the disclosure of the personal data is necessary for the organization to obtain legal services, consent is not required to be obtained by the organization from its data subject(s).

This is different under the GDPR. Under the GDPR, consent is one of the required legal grounds for processing personal information. However, the scope of consent is limited, and strictly defined.
The GDPR has clearly defined consent to be "**freely given, specific, informed** and **unambiguous** indication of the data the subject wishes by which he/her, by a statement or by **clear affirmative action**, signifies agreement to the processing of personal data relating to him/her."

The notion of "deemed consent" does not have similar traction under the GDPR as with the PDPA. As such, in all scenarios, organizations must take prudent steps to ensure that consent is clearly obtained.

Further, besides the requirement that consent must be given freely, the GDPR stipulates that even explicit consent may not be sufficient in cases where there is an imbalance of power, for example in the context of employer-employee relationships, or where consent to the processing of personal data is bundled together with other contractual provisions, particularly where such processing of personal data is not required for the performance of the contract. Employees are considered to be in a dependent situation in relation to their employers and may, therefore, be inclined to give consent whereas they might want to refuse. Consequently, when the processing has multiple purposes, consent should be given for all of them.

Organizations that have taken measures to remain compliant with the PDPA; this does not naturally equate to compliance with the GDPR. It is crucial that organizations in Singapore obtain valid consent from data subject(s) and be especially careful where the processing of personal data relies on "deemed consent" under the PDPA.

In addition, organizations must pay particular attention to scenarios under which consent for data collection, usage, or disclosure are exempted under the Second to Fourth Schedules of the PDPA, and there are no equivalent exemptions offered under the GDPR.

# Withdrawal of Consent

The withdrawal of consent by data subject(s) is permitted by both the GDPR and PDPA in varying degrees.

Under the PDPA, if the data subject(s) withdraws consent to the collection, use or disclosure of personal data the organization shall cease (and cause its data intermediaries and agents from doing so as well) collecting, using or disclosing the said personal data, unless, there was not a need to obtain consent from the data subject(s) in the first place (see above for the definition of "deemed consent" or exemptions under the Second to Fourth Schedules of the PDPA). The consequences of the withdrawal of consent should also be borne by the data subjects

However, upon the withdrawal of consent, the organization is not required to delete or destroy a data subject's personal data and may retain it for as long as there are necessary business or legal needs.

By contrast, under the GDPR, the data subject(s) shall have the right to withdraw his/her consent at any time. Upon the withdrawal of consent by the data subject(s), the organization should no longer process the personal data of the said data subject(s), unless another legal basis under Article 6 of the GDPR applies.

# Processing of Special Categories of Personal Data

Different categories of personal data are afforded different levels of protection. This is a concept that is present in the GDPR, but not in the PDPA.

Under the GDPR, special categories of personal data are defined as the "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."

The processing of special categories of personal data is generally prohibited under the GDPR unless the exceptions under Article 9(2) applies to the organization. These include: (i) processing of personal data which are made public by the data subject(s) (this exception is however interpreted vary narrowly); (ii) processing of the personal data is necessary to protect the vital interests of the data subject(s); or (iii) processing is necessary for reasons of public interest such as public health.

This is a marked difference from the position under the PDPA. The PDPA does not explicitly categorize personal data. Instead, limited guidance is provided by the Personal Data Protection Commission (the "**PDPC**") in its advisory guidelines, and adjudicated cases. The PDPC has highlighted that "*certain types of personal data would typically be more sensitive in nature*", without clearly demarcating what types of information would qualify as "*sensitive*" personal data. Nevertheless, an organization's obligations under the PDPA remain confined to ensuring that "*a higher standard of protection is implemented for more sensitive personal data*", as opposed to a prohibition from processing under the GDPR.

As a consequence, organizations now need to note the difference between general personal data and

special categories of personal data under the GDPR (and the consequent data processing prohibition). Given that the PDPA does not draw this distinction, it is likely that organizations will have to relook their internal procedures to accommodate this 'new' category of personal data.

## Data Breach Notification

The PDPA does not currently make it mandatory for organizations to notify the data subject(s) in the event there is a personal data breach. Instead, organizations are encouraged to notify individuals affected by the data breach

In comparison, under the GDPR, a data controller is obliged to report a data breach no later than 72 hours after such breach is discovered. In the event that there is a breach of personal data, the data controller is expected to document the said breach comprising of the facts in relation to the breach and any remedial actions taken.

The failure to adhere to this requirement may expose organizations to the same penalties described above. Organizations should take care to ensure that the relevant internal procedures are put in place to comply with this 72-hour timeline, particularly in light of the number of additional obligations imposed by the GDPR.

## Correction of Personal Data

Both the GDPR and the PDPA permit the data subject(s) to rectify his/her personal data in varying scenarios.

Under the PDPA, a data subject(s) may request to correct an error or omission in his/her personal data held by the organization. However, in Singapore, an organization is not required to comply with this request if it is satisfied on reasonable grounds that the correction should not be made.

Under the GDPR, the data subject(s) shall have the right to obtain data from the "controller without undue delay the rectification of inaccurate personal data concerning him or her." In addition, data subject(s) have the right to obtain from the controller without delay the rectification of inaccurate personal data concerning him/her. In the event that the personal data is incomplete, the data subject(s) shall have the right for it to be completed, including by means of providing a supplementary statement.

## Right to Access

Both the GDPR and PDPA entitle the data subject(s) to the option of access to his/her personal data.

Under the PDPA, data subject(s) may request personal data about him/her from the organization and how this personal data has or may have been used or disclosed within a year before the date of the request. Pursuant to the PDPA, the organization is not required to provide the information requested for matters

under the Fifth Schedule. For instance, (i) personal data which is subject to data privilege; or (ii) any opinion data that is kept solely for an evaluative purpose.

Additionally, the organization is not required to provide the requested information to the data subject(s) if it:

1. results in the threat of safety, physical, the mental health of a person other than the data subject;
2. results in immediate or grave harm to the safety, physical, mental health of the data subject;
3. reveals the personal data of another person;
4. reveals the identity of the person who provided the personal data of the data subject; or
5. be contrary to the national interest.

Under the GDPR, the data subject(s) shall have the right to obtain personal data from the controller including the right to obtain a copy of the personal data as long as it does not adversely affect the rights and freedom of others. Under the GDPR, the grounds for refusing a data subject his/her right to access is limited in comparison to the PDPA.

# Right to Object

There is no explicit right under the PDPA for a data subject to object to the processing of his/her personal data.

However, under the GDPR, the data subject has the right to object to the processing of his/her personal data. Upon the objection of the data subject, the data controller should no longer process the personal data unless there are 'legitimate compelling reasons' to do so.

# Conclusion

As seen above, the GDPR marries a rigorous approach to data protection with an ambitious territorial scope.

It remains to be seen how the GDPR's enforcement will be implemented. However, given the intended global reach of the GDPR, it would be prudent for organizations to revise their internal procedures and data protection policies to address the additional obligations imposed by the GDPR, over and above the existing requirements of the PDPA.

# Disclaimer

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is for information purposes only, and not intended to provide legal or any other advice, or to be relied on in any way.

Neither AKD Benelux Lawyers nor CNPLaw LLP shall be liable for any loss, damage or other consequences arising from any reliance on the contents of this publication. In the event that you have any queries about the operation of the GDPR or the PDPA, you can and should seek your own legal advice.