

LEGAL  
ALERTSingapore  
22 March 2018

## Author

## Gregory Chan

Director  
ZICO Insights Law LLC  
[gregory.chan@zicolaw.com](mailto:gregory.chan@zicolaw.com)

## Ho Li-Ling

Senior Associate  
ZICO Insights Law LLC  
[li.ling.ho@zicolaw.com](mailto:li.ling.ho@zicolaw.com)

## The Impact of the EU GDPR in Singapore

The European Union General Data Protection Regulation (“EU GDPR”), which will enter into force from 25 May 2018, will apply to a Singapore organisation that processes personal data of individuals in the EU, where such processing relates to an offer of goods or services to individuals in the EU (regardless of whether payment is required) or the monitoring of the behaviour of individuals in the EU. Depending on its operations, an organisation in Singapore may therefore be required to comply with the EU GDPR in addition to its existing obligations under the Personal Data Protection Act 2012 (“PDPA”) of Singapore.

Factors such as the use of a language or currency that is generally used in one or more member states of the EU, with the possibility of ordering goods or services in that language, would be relevant in ascertaining whether the organisation is offering goods or services to individuals in the EU.

Where the EU GDPR is applicable, a Singapore organisation may be required to appoint a legal or natural person as its representative in an EU member state. However, it is not necessary for a Singapore organisation to do so if the processing of personal data by it is only occasional and does not include the large scale processing of special categories of personal data.

Under the EU GDPR, personal data is any information that relates to a natural person or data subject that can be used to directly or indirectly identify that person. Such information can include a name, a photo, an e-mail address, bank details, posts on social media websites, medical information, or a computer IP address.

This legal update seeks to provide an overview of the key obligations of Singapore organisations under the EU GDPR.

### Purpose and data minimisation

The EU GDPR requires that personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The EU GDPR mandates that only personal data that is necessary for the purpose can be collected and the personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or further processed.

### Basis of processing

There are several situations where the processing of personal data is lawful under the EU GDPR. For example, the processing of personal data complies with the EU GDPR if the individual has given consent for the processing for one or more specific purposes, or if it is necessary for the performance of a contract or for the organisation’s compliance with a legal obligation or it is necessary to protect the vital interests of the individual or another natural person.

### Consent

Unlike Section 15 of the PDPA, which allows Singapore organisations to rely on deemed consent, the GDPR does not appear to permit the concept of deemed consent at all. Under Article 4 of the EU GDPR, for an individual to have given consent under the EU GDPR, he or she must have provided a freely given, specific, informed and unambiguous indication of his or her agreement to the processing of his or her personal data.



## Rights of individuals

The EU GDPR requires organisations to provide certain rights to individuals, such as the right to access and obtain a copy of the individual's personal data, the right to erase or restrict the processing of personal data concerning the individual in certain circumstances, the right to rectify inaccurate personal data, as well as the right to data portability by receiving personal data concerning the individual which he has provided to the organisation, in a structured, commonly used and machine-readable format, and the right to transmit that data to another organisation.

## Responsibilities of organisations

Apart from designating a data protection officer in certain cases, such as where the organisation's activities involve regular monitoring of individuals or processing special categories of personal data, the responsibilities of organisations under the EU GDPR include implementing appropriate measures to ensure that, by default, only personal data that is necessary for the specific purpose is processed and assessing the impact of processing on the protection of personal data in certain circumstances, including where the processing is likely to result in high risk to the rights and freedoms of individuals.

## Personal Data Breach and Administrative Fines

Under the EU GDPR, in the event of a personal data breach, an organisation must notify the relevant supervisory authority in the EU without undue delay and where feasible, not later than 72 hours after becoming aware of the breach. Further, the organisation is also required to notify the individual concerned, without undue delay, if the personal data breach is likely to result in a high risk to the rights and freedoms of the individual. As the timeline for an organisation to notify the relevant regulatory authority and individuals is very short, organisations should develop a robust system for addressing security incidents and making the necessary reports under the EU GDPR.

Like the PDPA, the EU GDPR exerts extraterritorial reach. Depending on the provisions infringed upon, administrative fines of up to EUR10 million or 2% of its worldwide annual turnover of the preceding financial year (whichever is higher), or up to EUR20 million or 4% of an infringing organisation's worldwide annual turnover of the preceding financial year (whichever is higher), may be imposed by the supervisory authority of the relevant EU member state.

## References

The Personal Data Protection Commission ("PDPC") published a fact sheet on its website on 4 October 2017 which highlights the key requirements of the EU GDPR applicable to organisations in Singapore. The fact sheet is available from the website of the PDPC at [www.pdpc.gov.sg](http://www.pdpc.gov.sg).

For more information on the EU GDPR, please refer to the EU GDPR text and the resources issued by the European regulators on the interpretation of the EU GDPR.

If you have any questions or require additional information, please contact [Gregory Chan, Ho Li-Ling](#) or the ZICO Insights Law LLC partner you usually deal with.

[www.zicolaw.com](http://www.zicolaw.com)

---

*This alert is for general information only and is not a substitute for legal advice.*