European Union
General Data Protection Regulation
Factsheet for Organisations

The European Union General Data Protection Regulation (EU GDPR)[1] replaces the EU Directive[2] and will enter into force from 25 May 2018. The EU GDPR will apply to an organisation established outside of the EU, so long as the organisation offers goods or services to individuals in the EU, or monitors their behaviour within the EU. This includes any organisation processing and holding personal data of individuals residing in the EU, regardless of the organisation's location.

KEY REQUIREMENTS OF EU GDPR	
Application of EU GDPR (Articles 3 & 27)	The EU GDPR applies to any organisation that processes personal data of individuals in the EU, including organisations established outside of the EU, where the processing relates to: a) offer of goods or services to individuals in the EU (regardless of whether payment is required); or b) monitoring of the behaviour of individuals in the EU. Considerations for ascertaining whether the organisation is offering goods or services to individuals in the EU would include the use of a language or currency that is generally used in one or more EU Member States, with the possibility of ordering goods and services in that language[3]. Where the EU GDPR applies to an organisation not established in the EU, the organisation may be required to appoint a representative[4] in an EU Member State. An EU representative is not required to be appointed where the processing by an organisation is only occasional and does not include processing of special categories[5] of personal data on a large scale.
Basis of processing (Article 6)	Under the EU GDPR, processing of personal data is lawful[6] if – a) Consent[7] is given by the individual for the processing for one or more specific purposes; b) It is necessary for the performance of a contract;

[1]Regulation (EU) 2016/679 of the European Parliament and of 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.

[2]Directive 95/46/EC of the European Parliament and the Council of 24 October 1995.

[3]Recital 23 of the EU GDPR.

[4]A representative means a natural or legal person established in the EU who is designated by writing by the organisation to represent the organisation in the EU.

[5]Special categories of personal data include racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union or membership; processing of genetic data; biometric data for uniquely identifying a natural person; data concerning health; data concerning a person's sex life or sexual orientation.

[6]The following bases do not apply to the processing of special categories of personal data, which is generally prohibited except in very limited circumstances (e.g., where the processing relates to personal data made public by the individual).

[7]Consent of the individual means any freely given, specific, informed and unambiguous indication of the individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of his or her personal data.

	c) It is necessary for the organisation's compliance with a legal obligation; d) It is necessary to protect vital interests of the individual or another natural person; e) It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation; or f) It is necessary for the purposes of legitimate interests.
Rights of individuals (Articles 15, 16, 17, 18, 20, 21 & 22)	The EU GDPR provides a number of rights to individuals that organisations will have to provide – **a) Right to access** and obtain a copy of the individual's personal data, including the purposes of processing and who the personal data has been disclosed to; **b) Right to rectification** of inaccurate personal data concerning the individual; **c) Right to erasure** of personal data concerning the individual in certain circumstances; **d) Right to restriction of processing** in certain circumstances, such as where the accuracy of the personal data is contested, or the processing is unlawful; **e) Right to data portability** by receiving personal data concerning the individual or data 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; **f) Right to object** to the processing of personal data in certain circumstances, including for the purposes of direct marketing; and **g) Right not to be subject to automated decision-making (including profiling)** where this has legal effect on the individual or significantly affects him.
Accountability and governance (Articles 25, 35 & 37)	Responsibilities of organisations include – **a) Data protection by design and by default** – Implementing appropriate measures to ensure that, by default, only personal data that is necessary for the specific purpose is processed; **b) Data protection impact assessment** – Carrying out an assessment of the impact of processing on the protection of personal data in certain circumstances, including where the processing (particularly the use of new technologies) is likely to result in high risk to the rights and freedoms of individuals; and **c) 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.

Data breach notification (Articles 33 & 34)	In the case of a personal data breach, the organisation must – a) Notify the supervisory authority without undue delay, but not later than 72 hours where feasible; and b) Notify the individual without undue delay, if the personal data breach is likely to result in a high risk to the rights and freedoms of the individual. A data processor must also notify the organisation without undue delay after becoming aware of a breach.
Administrative fines (Article 83)	Depending on the provisions infringed upon, the following administrative fines may be imposed – a) Up to 10 million EUR or 2% of worldwide annual turnover of preceding financial year (whichever is higher); or b) Up to 20 million EUR or 4% of worldwide annual turnover of preceding financial year (whichever is higher).

This document is intended to highlight key aspects of the EU GDPR to organisations in Singapore, and does not provide an interpretation of the EU GDPR. 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 GDPR (e.g., EU's Article 29 Data Protection Working Party Guidelines on the right to data portability, data protection officer and data protection impact assessment). Where further assistance is required, organisations may wish to seek professional legal advice to ensure compliance with the EU GDPR.