Data Protection Legislation

Introduction

The Personal Data Protection Act ("PDPA") establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. The PDPA is administered and enforced by the Personal Data Protection Commission ("PDPC") of Singapore.

The General Data Protection Regulation ("GDPR") is an European Union ("EU") regulation that applies to and regulates the standards of data users or data processors who process Personal Data of EU natural persons ("Individuals") by data users or processors regardless whether the processing takes place in the EU. It is being enforced by the European Commission ("EC").

Overview of Key Regulatory Obligations

Key Legislation for PDPA and GDPR

The following table covers the key legislation that governs the PDPA and GDPR.

Key Legislation	PDPA	GDPR
Qualification Grounds		
Date of Commencement	2 July 2014	25 May 2018
Jurisdiction Territoriality	**Applies to Singapore –** Personal data in Singapore is protected under the PDPA.	**Applies Globally –** Applies to and regulates the standards of data users or data processors who process personal data of EU natural persons regardless of whether the processing takes place in the EU.
Scope of Data	**Personal data –** The PDPA applies to any data in which an individual can be identified from that data.	**Identifiers –** The GDPR applies to any information allowing an identifiable natural person to be identified.
Personal Data Processing Obligations When Collecting Personal Data		
Consent	**Consent before collection –** The individual must give consent for the collection, use or disclosure of personal data to the organisation for purposes as disclosed.	**Consent before collection –** Before personal data is collected, the Individual must first give his consent for his personal data for the prescribed purpose(s). Conditions for obtaining consent such as the ability to demonstrate that the Individual consents must be met before the consent can be valid. Where personal data is not collected directly from the Individual but from a third-party source, the Controller will need to inform the Individual, the details of the Controller who maintains this personal data.

Qualification Grounds

Obligations When Collecting Personal Data

Purpose Limitation

Obligations when Storing Personal Data

Obligations when Transferring Personal Data

Key Legislation	PDPA	GDPR
Personal Data Processing Obligations When Collecting Personal Data		
Purpose Limitation	**Collected for specific purposes –** Where personal data is collected, it must be collected only for purposes which have been disclosed to the individual or that a reasonable person would consider appropriate in the circumstances.	**Collected for specific purposes –** Where personal data is collected, it must be collected for specified, explicit purposes which are not incompatible with its initial purposes. This limitation does not extend to further processing for archiving for public interest, scientific, historical research or statistical purposes The collection of personal data should be limited only to the objective of its initial purposes .
Personal Data Processing Obligations When Storing Personal Data		
Accuracy	**Quality personal data –** The personal data collected will need to be kept accurate and up to date having regard to its initial purpose.	
Time Limitations	**Personal data lifespan limited by purpose –** Personal data must be kept in a form which permits the identification of natural persons for no longer than is necessary for its initial purpose. Personal data that is in record for at least 100 years shall not apply and personal data about a deceased individual shall not apply.	**Personal data lifespan limited by purpose –** Personal data must be kept in a form which permits the identification of natural persons for no longer than is necessary for its initial purpose. This limitation does not apply to storing personal data for archiving for public interest, scientific, historical research or statistical purposes.
Security Obligations	**Protection obligation –** Reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.	**Obligations to protect personal data –** Measures must be taken to ensure the security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.
Personal Data Processing Obligations When Transferring Personal Data		
Transfer Limitations	**Transfers of personal data to outside of Singapore –** Organisations must not transfer any personal data outside Singapore except when requirements prescribed under the PDPA are met to ensure that organisations provide a standard of protection to personal data that is comparable to the protection under the PDPA.	**Transfers of personal data to outside the European Union –** A Controller must ensure that any transfer of personal data which are undergoing processing or are intended for processing after transfer to a country outside the union or to an international organisation shall take place only if the obligations for data protection under the GDPR have been met.

Transfer Limitations

Delegation Limitations when Dealing with Personal Data

Key Legislation	PDPA	GDPR
Personal Data Processing Obligations When Transferring Personal Data		
Transfer Limitations	**Personal Data Protection Commission decision –** The Commission may, on the application of any organisation, by notice in writing exempt the organisation from any requirement to provide data protection comparable to the protection under the PDPA outside of Singapore in respect of any transfer of personal data by that organisation.	**European Commission decides which countries are cleared for transfer –** A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation. In the absence of a decision by the Commission, a Controller or processor may transfer personal data to a third country or an international organisation only if the Controller or processor has provided appropriate safeguards, and on condition that the individual's right, legal remedies and safeguards are in place.
Personal Data Processing Obligations When Dealing with Personal Data		
Delegation Limitations	**Responsibility –** An organisation shall designate individuals to be responsible for ensuring that the organisation complies with the PDPA. The organisation is ultimately responsible for personal data in its possession or under its control.	**Data protection under delegation –** Where processing is to be carried out on behalf of a Controller, the Controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures. **EU Legal contract for delegation –** Processing by a processor shall be governed by a contract or other legal act under EU law and the processor must be capable to be bound under EU law and indicate the strict terms as required under the GDPR that ensures the processor's compliance to the GDPR. The processor must be made contractually subject to the same data security obligations of the Controller under the GDPR.

Record Keeping

Personal Remedies

Key Legislation	PDPA	GDPR
Personal Data Processing Obligations When Dealing with Personal Data		
Record Keeping	**Data protection –** General rules with respect to protection, collection, use, disclosure and retention of personal data are not imposed on a data intermediary in respect of its processing of personal data on behalf of another organisation.	**Duty to keep records of processing activities –** Each Controller and, where applicable, the Controller's representative, shall maintain a record of processing activities under its responsibility.
Personal Remedies Against Data Controllers and Processors		
Access to Personal Data	**The Individual's right to access –** The organisation shall provide the individual with access to personal data as soon as reasonably possible.	**The Individual has a right to access and obtain a copy** of the individual's personal data, including the purposes of processing.
Disclosure of Data handling	**The Individual has a right to obtain disclosure –** The organisation shall upon request, within a reasonable period provide information to the individual about personal data that is under its control.	**The Individual has a right to obtain disclosure** on who the personal data has been disclosed to, where it is stored, and the period for which it is stored.
Rectification of Personal Data	**The Individual has a right to request amendments –** The organisation shall upon request, make amendments to the personal data unless there are restrictions.	**The Individual has a right to rectification** of inaccurate personal data concerning the individual.
To be Removed, Erased or Forgotten	**The Individual has a right to demand for erasure –** The organisation shall upon request, remove the means by which the personal data can be associated with particular individual unless there are restrictions.	**The Individual has a right to demand for erasure** of personal data in certain circumstances, such as where the personal data is no longer necessary for its collection purposes, where the individual withdraws consent and the Controller has no legitimate grounds to keep the data, where the personal data has been unlawfully processed.

Personal Remedies

Key Legislation	PDPA	GDPR
Personal Remedies Against Data Controllers and Processors		
Restrictions on Processing	Nil	**The Individual has a right to restrict** the processing of personal data in certain circumstances, such as where the accuracy of the personal data is contested, or the processing is unlawful. **The Individual has a right to object** to the processing of personal data at any time in certain circumstances, including for the purposes of direct marketing. **The Individual has a right to be subject to automated decision-making** (including profiling) where this has legal effect on the individual or significantly affects him.
Portability, Movement and Exit options	**Nil**	**The Individual has a right to data transportability** 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.
Notifications	**The Individual has a right to obtain disclosure be notified of breach** – When there is personal data breach, the Controller/organisation shall communicate the personal data breach to the data subject without undue delay.	
Direct Remedies	**The Individual has a right to be compensated –** Individuals who suffer loss or damage as a direct result of a contravention of part of the PDPA may commence civil proceedings in the courts against the organisation.	**The Individual has a right to be compensated –** Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the Controller or processor for the damage suffered.

Data Protection Representatives

Data Protection Officers

Key Legislation	PDPA	GDPR
Strict Liabilities, Accountability and Governance		
Representatives	**Nil**	**Designation of a Representative –** The Controller or the processor shall designate in writing a representative in the EU (the "Representative") in certain cases, such as where the organisation's activities involve regular monitoring of individuals or processing special categories of personal data. The representative shall be established in one of the Member States where the data subject's personal data is being monitored. The Representative shall also be responsible for the compliance to the GDPR.
Data protection officer	**Data Protection Officer –** Organisations are required to designate at least one Data Protection Officer, to oversee the data protection responsibilities within the organisation and ensure compliance with the PDPA.	**Designation of a Data Protection Officer –** The Controller will in certain cases such as where the core activities of the Controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of EU nationals on a large scale. The Data Protection Officer role is to advise the Controller or Processor, monitor the compliance by the Controller of the processor to the GDPR, inform and educate the Controller or the Processor and its employee's on GDPR obligations and to co-operate with the authorities.

Key Legislation	PDPA	GDPR
Strict Liabilities, Accountability and Governance		
Data Protection Policies	**Policies –** Organisations are required to develop and implement policies and practices that are necessary to meet its obligations under the PDPA. Data protection impact assessment can be carried out in order to take a proactive and systematic approach in adopting appropriate measures and tools to address specific personal data protection risks and organisational needs.	**Data protection by design and by default –** The Controller must implement appropriate measures to ensure that, by default, only personal data that is necessary for the specific purpose is processed. Only when the Controller has adhered to a code of conduct approved by the GDPR then he can demonstrate compliance with the obligations of a Controller under the GDPR. **Data protection impact assessment –** A Controller needs to carry 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 seek advice.
Supervisory Authorities	**Duty to Notify Authorities –** In the consulting paper in response to the feedback on public consultation on 1 February 2018, PDPC proposed that organisation must notify PDPC of a data breach that poses any risk of impact or harm or the scale of the data breach involving 500 or more affected individuals.	**Duty to Notify Authorities -** In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.
Strict Liabilities, Accountability and Governance		
Penalties for Breach	**Fines –** Infringements of the PDPA in certain cases, such as evading a request under access or correction of personal data shall attract administrative fines of up to SGD5,000. Or in any other case, to a fine not exceeding SGD50,000.	**Fines -** Infringements of the GDPR in certain cases, such as certification of Personal Data protection and the failure to implement data protection by design and default shall, attract administrative fines up to EUR10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Penalties of Breaches

Key Legislation	PDPA	GDPR
Strict Liabilities, Accountability and Governance		
Penalties for Breaches	Infringements of the PDPA in obstructing, hindering or furnishing false or misleading in any material particular, such as evading a request under access or correction of personal data shall attract administrative fines of up to SGD10,000 or to imprisonment for a term not exceeding 12 months or to both. Or in any other case, to a fine not exceeding SGD100,000.	Infringements in certain cases, such as the rights of the individual or non-compliance with an order by the supervisory authority attracts up to administrative fines up to EUR20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Vistra – PDPA + GDPR Services

Vistra can review the current processes in data protection and perform the necessary remediation work to bridge the gaps in current data protection controls in accordance with the PDPA or GDPR requirements. For new or existing entities, Vistra can provide or review the relevant data protection policy and implement it for the entity.

Vistra can also provide a consultant who is experienced in personal data protection compliance requirements. The appointed consultant will act as the entity's Data Protection Officer ("DPO"), providing support and advice upon demand.

The DPO will work with the entity to implement processes to improve the areas which have been identified as having weaker controls in accordance with the PDPA or GDPR requirements. The scope includes the following:

- Provide a customised privacy statement for the entity to be displayed on their website and other points of collection of personal data.
- Perform updates on the control list which contains information such as data storage facilities, access controls and password controls, etc
- Advise the entity on the required information to be transparent with the public.
- Communicate to staff regarding the importance of personal data protection and procedures to adhere to regulatory requirements.
- Perform regular risk and process assessment to determine the risk controls as well as the integrity of internal process regarding personal data protection (the assessment will be scaled towards the size and complexity of the business).
- Interact with persons inquiring about their personal data, including requests for disclosure and correction.
- Perform the necessary check to determine if personal data can/will be deleted from the storage facility of the entity.
- Management of complaints from persons.

Most importantly, the DPO will work with the entity to implement the necessary adjustments to the business to work towards compliance with the PDPA or GDPR requirements.

Action Required

It is essential that Singapore entities review their current data protection situation and appoint a DPO to ensure compliance with the PDPA, which is a law that applies to all entities' collection, use and disclosure of personal data in Singapore.

Please contact your Vistra representative or singapore@vistra.com if you would like to enquire more about our data protection services.